2000

Internet Protocol version 6 and the future of home networking

Laurie Blumsack

Laurie Blumsack

Internet Protocol Version 6 *and the* Future *of* Home Networking

Master of Science
Information Technology
Thesis
January 2000

Master of Science in Information Technology

Capstone Project/Thesis Approval Form

Student Name: Laurie Blumsack

Student Number:

Project/Thesis Title: IPV6 and the future of Home Networking

Project/Thesis Committee:

Name	Signature	Date
Jeff Lasky		March 13, 2000
Chair		
Sylvia Perez-Hardy		March 13, 2000
Committee member		
Bruce Hartpence		3-13-00
Graduate Program Chair		

Table of Contents

Abstract

Home networking will be more of a necessity in the future than it is today. The homes of the future will make our lives easier in many ways. As microprocessors become less expensive and require less power they will be implanted into many of the common household items used everyday. Appliances and components will evolve into smart devices that communicate with each other. Connecting these devices will become more important as devices incorporate new technologies. It will be necessary to build a network that can handle the needs of this type of computing environment.

The home networks of the future will require many of the same features that can be found in today's corporate networks. However, there will be four issues that will determine the level of success of implementing home networks. The first issue is the increase in volume of the devices accessing and utilizing the Internet. Security will be a high priority for homeowners, since the data that accumulates and circulates in and out of the home is sensitive and personal. The third critical issue is ease of use, because the average homeowner does not have the skills necessary to configure and maintain networks. The last issue that will be important in the home is the increased need for bandwidth and the ability to accommodate all types of data traffic.

There is no doubt that the Internet Protocol will be important in future home networks. Some proponents of IP say "IP over everything" The trend has been finding new ways of making IP the answer to all types of voice and data communications. Initially the Internet Protocol was designed for a specific application. Over time, IPv4 has been able to successfully adapt to the changing needs and demands of the Internet. At one point in the early 90's, it was feared that IPv4 would not be able to meet the future

needs. As a result, The Internet Engineering Task Force (IETF) developed a next generation Internet Protocol, referred to as Internet Protocol version 6. In the meantime, new fixes to old IPv4 problems have been temporarily halted. The implementation of IPv6 has been extremely slow since the imminent danger of declining address space has been temporarily addressed.

IP version 6 has many new features built into the protocol that will streamline and enhance many aspects of the network, but these features alone may not be enough to cause the displacement of the massive infrastructure of IPv4. Will IPv6 be better at handling the demands of the home networks of the future, or will the additions and updates for IPv4 be sufficient? What are some of the resolutions that are being developed or are already implemented for the key issues in home networks- the increasing number of devices, security, ease of use and data flow?

Introduction

When devices start to think, the way we interact with everything around us will change. Our homes will change as well. Homes will no longer be isolated from the rest of the world; they will be integrated into the ebb and flow of information exchange. Our microwaves, toasters and home security systems will be internetworked with our Personal Digital Assistants and other mobile communication devices.

How will all these devices be managed when everything around us is networked? Microprocessors will be a key component in this evolution. Microprocessors will have the ability to store and process the details of our lives. Microprocessors can be placed in the appliances we use everyday, such as the refrigerator and microwave. By doing so,

new functionality can be added to create user friendly and interactive objects. Data in itself is valuable, but when data is shared the value is increased.

One protocol that has the ability to share data across all types of networks is the Internet Protocol. IP addresses the issues of millions of PC's and devices with different operating systems and platforms communicating with each other. The Internet Protocol is able to translate or mediate whatever form of information it receives, regardless of what media (copper wire, optical fiber, wireless) or service (native IP, frame relay, ATM) it may run on. Some examples of the types of network situations mediation handles include:

- Incompatible client/server software.
- Incompatible LAN environments (i.e., Windows and Unix).
- Different communications systems (i.e., IP and Plain old telephone system (POTS).
- Different QoS mechanisms (i.e., IPv4, IPv6, and ATM).
- Different bandwidth capabilities (i.e., caching, mirroring, load distribution).

This mediation capability was built into the TCP/IP (Transport Control Protocol) protocol suite from the start. As a platform-independent set of standards, TCP/IP bridges the gap between dissimilar computers, operating systems, and networks. It is supported on nearly every computing platform, from PCs, Macintoshes, and Unix systems to thin clients and servers, legacy mainframes, and the newest supercomputers. In supporting both local and wide area connections, TCP/IP also provides seamless interconnectivity between the two environments (Muller, 1998). IP lets computers link to one another without having to know anything more than an address. It is the cornerstone of the Internet and will be an excellent cornerstone for the home networks of the future.

Home networks will grow and evolve over time. It is important to not assume everything that needs to be invented to make home networking a reality has already been invented (Mouhanna, 1999). There may be dozens of new devices that are developed. There will be new applications and new ways of handling information. IP will definitely be a part of home networks, but as the needs and conditions change the protocol will have to continue to evolve. There are two possibilities. The first possibility is that IPv4 remains the dominant protocol and IPv6 never gets off the ground. The second scenario is that IPv4 will be slowly transitioned over to IPv6. In either case, new issues will continue to surface and new solutions will be created. Which protocol will have greater potential for expansion? Was it worth the efforts of the Internet Engineering Task Force to create IPv6?

This thesis will attempt to answer the question about which version of IP will be the best suited to manage the data flow created by the devices in homes in the future. Home networking is an application of a protocol that doesn't currently exist on a large scale, so it will be necessary to understand what will exist in a home network. Each component of the system will create different needs to address. It is no longer the issue of PC's connected to printers and other printers on the network, it is the issue of connecting smart devices to each other.

Current Scenario

Home networking has been receiving attention lately because there are new protocols and standards that have been the result of an industry wide effort. More homes today contain multiple personal computers than ever before. Slowly, owning a home personal computer has become the norm in technologically advanced societies. In the

United States alone there are more than 18 million homes that have more than one personal computer (Solomon, 1999). In 1999, the U.S. Government census statistics stated that about 30 million of the approximately 100 million households in the U.S. have Internet access devices (Muller, 1999). Some projections indicate that as many as 47 percent of households will have Internet access devices by 2002 (Muller, 1999). Although these estimates may be optimistic, the trend remains the same- homes connecting to the Internet are on the rise.

As more and more computers are placed in the home, the need to network these devices will increase. These computers will not be isolated- they will be connected to each other and to the Internet. The other trend is a surge of information appliance products that will be entering the market. United States shipments of smart appliances are expected to out number desktop personal computers by 17 percent in 2001 (Reuters, 1998). It will no longer be one or two PC's in the home, but dozens of smaller independent devices with individual functionality. The key will be how to connect all of them.

There are systems on the market today that provide a glimpse of tomorrow. IBM offers a product called Home Director, which has a TV interface and uses a server that manages sensors and components that are placed throughout the home (Huffstutter, 1998). With a single remote, the heating and cooling systems can be adjusted, the VCR can be programmed, the lights can be turned off and on, and other remote systems can be monitored (Huffstutter, 1998). There are many other manufacturers and service providers that are in the process of developing similar products and systems. This is only the beginning.

Ubiquitous Environments

The ultimate goal in a home is to achieve a ubiquitous computing environment. We eat, sleep and relax in our homes. We watch TV, we cook meals, we clean and do the laundry, we connect and communicate with our family and friends, we spend time on the Internet, and we rest in our homes. A home is a place where we can be ourselves and a place where we can express who we are. It is a place where people go to spend time with family and friends. People are always trying to find ways to simplify their life and make tasks less difficult. If humans can harness the capabilities of microprocessors, our lives may be less complicated and more fulfilling. The person who is interacting with them shouldn't be fully cognizant of their presence. In many ways interacting with a computer today requires learning a new language and using foreign tools, such as a mouse. Eventually the PC's around us will become much more user friendly. Speech recognition and text to speech software will truly enhance our ability to interact with computers in a seamless manner.

In order to create a seamless computing environment, it is necessary to have a ubiquitous system of devices. The concept of ubiquitous computing, which was coined by Mark Weiser, previous chief technologist at Xerox PARC, is very simple. Instead of one computer sharing many people, there are many computers sharing one person (Wasserman, 1998). The technology should be transparent and highly distributed. Electronic systems will be merged with the physical environment to provide computer functionality to everyday objects (Cooperstock, 1997). Weiser also stated that the computer designs of the future should allow people to remain serene and in control, and creating an environment of calmness is the ultimate goal (Weiser, 1997). This is already

starting to happen around us. There are more and more devices that have embedded computers in the present world. For example, a new Tonka truck has been introduced that responds to voice commands. It isn't magic, it is an embedded microprocessor. Cars, microwaves and the singing greeting cards all have minicomputers. Unlike these things, most of us are aware we are using computers because a majority of the computers we deal with today are not intuitive, nor are they transparent. Most computer interaction requires boot up, a huge monitor for feedback and a keyboard for input. Significant cognitive activity is required for a majority of human-computer interaction today. However, tomorrow may not be so mentally challenging.

Home system will always know where everyone is and what their preferences are for any given situation. Ubiquitous computing means that your day and environment would be extremely personalized. This is what makes the ideal state of ubiquitous computing so difficult to achieve. Transparency is the key to success. If humans are distracted by the technology or negatively affected by computers, it will never be allowed into our homes. In order to achieve ubiquitous computing it is necessary to create a completely networked environment. All of the computers that surround us will need to be networked in order to function and communicate commands. Nothing will work as a stand-alone device because the ability to gather and share information can create new ways of doing things. The potential is too powerful to ignore. In addition, without the ability to gather information it is nearly impossible to achieve a ubiquitous environment.

Homes in the future

Microprocessors will continue to be faster and cheaper. New uses will continue to appear every day, and we won't even be cognizant of the fact that these components

will be in our homes. Desktop computers will transform from being a single unit into a number of different devices with different functionality. For example, instead of booting up a PC to check the weather, a separate device will maintain and display updated weather reports data. There may be a separate device for mail and another device for games. Computing will no longer be housed in a single unit, but rather multiple units placed or accessed throughout the home. These specialized devices will continue to improve in functionality. Some devices will be a portal to the rest of the world. They will continue to change in shape, function and complexity.

Simplicity is the key. If the devices are perceived as complex machines that require skills not commonly available to most people, they will not be adopted (Venkatesh, 1996). Consumers of every age, intelligence and size should be able to manage all of the components in a household. Manuals should be banned. The human-computer interaction should be seamless. The days of frequent error messages and hung computers should be a distant memory before the home becomes a place for digital appliances of every shape, size and function.

How far will the home of the future be from where we are today? We still need entertainment, we still need to relax, eat, and clean our clothes. Established behaviors don't suddenly change when new technology is introduced, the technology will have to adapt to the way people are already behaving in the home environment (Greenberg, 1997). The appliances and devices that are introduced should be able to accomplish the same tasks we do today. It is safe to say that smart appliances and devices, if successful at all, will slowly emerge and evolve over a long period of time. It may be several generations before the remnants of the 20th century fade away. In the mean

time, progress will be slow. The day, however, will arrive when technically enhanced homes are a reality.

The Living Room

The living room should be a place that reflects its name- a place to live. This room will continue to be filled with family and entertainment. The television will no longer be a passive box. It will be a combination of broadcast channels and the Internet, movie rental store and the movies. Viewers in all countries around the world will be able to pick programs from the global market (Cairncross, 1997). The programming list will be very long, and will be browsed by powerful search engines. Movies will be downloaded and programs will be retrieved on demand. People will be able to manage every aspect of their entertainment schedule. There may be other individual "televisions" but they will be secondary and not located in the same room as the primary television, as they are today.

Although some may argue, there will probably be a separate gaming or interaction station in addition the future television. This entertainment system will be similar to the PC but only focused on providing entertainment. It will be a distant relative of the television and it will resemble the World Wide Web, as we know it today. It may be a room or a place to go to experience some version of virtual reality or it may be a set of mobile headsets. By 2017, some experts forecast that watching a movie will no longer mean relaxation, but rather an interactive, virtual world of the story (Greenberg, 1997). Whatever it is, it will be separate from the other systems in the home and will probably require the most bandwidth and multimedia capabilities. It is a separate unit because it is difficult to believe that personal systems will have the power and

interactivity that is needed for this high level of activity at this point in time. However, this entertainment center is only the intermediary step to eventually having personal systems that will have enough processing power to perform any activity every day.

Multiple remote controls will be a thing of the past. The controlling mechanism could either be a part of the personal digital assistant, or it could be a voice activated system that is part of the system as a whole. It could also be a mixture of both depending on your mood and preference.

The stereo and radio will also transform into a system that will be more powerful. They will no longer simply be a dumb receiver and tuner, it will have more intelligence and offer a plethora of options and variety. Instead of separate units piled on top of one another, it will be integrated into the rest of the system. The likely source for music and programming will be the Internet. Entertainment programs will be designed for the individual, not for the masses. CD's will be remembered along with the vinyl albums. In other words, the music won't need to be stored in the home. It will be accessed remotely, on demand. The music and audio components will be able to sense when to turn down the volume or turn off, based on the other activities that are going on in the environment. It will all be a part of the larger system, no longer a stand-alone device.

Artwork will also be part of the changing scenery. Flat panel monitors could display the art of the day. The artwork could be subscribed to just like a weekly magazine. It could change depending on who is in the room or who is visiting. Imagine furniture or carpeting having the same ability (Greenberg, 1997). It could change color or patterns based on the day of the week or the color of clothes you are wearing.

The Kitchen

As for the kitchen, it will no longer require an intensive search prior to visiting the grocery store, because the kitchen will know what it has in stock, and what is needed to prepare the meal. Everything will be tagged so that the refrigerator and the grocery store can track it. Coupons can be obtained on-line. Food preparation will be a lot less confusing because the recipe will be easily displayed on a monitor that was found by searching a global cookbook. By inputting the number of people to the system it will automatically adjust the recipe and all of the ingredients can be checked against the inventory. There will be sensors that determine the status and databases that store recipes and preferences. The oven will be preheated and all of the cooking devices will notify you when they need to be turned on. Microwaves and toasters and coffee makers will join the fuzzy logic rice cookers and bread makers of today. They will all have microprocessors that help even the most inept chefs make fantastic meals. NCR, a British Company, did intensive research, and they believe that the kitchen offered the best possibility for introducing the masses to networked living (Huffstutter, 1998).

Bedrooms and Bathrooms

Bedrooms and bathrooms will be wired just like the rest of the house. Alarms will be designed and programmed to wake you up the way you prefer. Each piece of clothing may have its own microprocessor. Your clothes will be able to communicate to you when they were last washed and worn, and what looks best in combination with it. Watches will be able to set themselves, and jewelry boxes can have their own security. Makeup and toiletries can also be tracked in the same manner as food. The curling iron could turn itself on when you start the shower. The electric razor can notify you that a new razor is needed. This is only the beginning.

Laundry rooms will also be a potential place for microprocessors. The clothes can notify the washing machine what the best cycle and temperature is, and if you accidentally mix in a dark with the light it will warn you of the impending disaster. In addition, the sneakers or shoes that you wear can provide enough energy to power a smaller personal network. Shoes could contain a small tracking device or transmitter so that the person wearing them can always be found.

Communications

A person who likes to start their work day off first thing can have their high priority emails waiting to be read to them the minute they put their feet on the floor. As they move the house, the system would know to "follow" the email report throughout the house. If they weren't finished by the time the person was ready to leave, the remaining messages could be transmitted to the car (Thomas, 1997).

The telephone will also need to be a part of the system, but in a whole new way. Eventually, video conferencing will enter our lives. Mobile phones will become more and more common. Answering machines will be far more powerful than they are today. The messages will be accessible from anywhere and in any format, by any authorized user.

There will continue to be home offices that will require the same level of service that is available in the business office. Whether or not people will be telecommuting is not the issue. The issue is that the requirements to do business from the home will be the same as at the office. People will no longer accept dial up speeds; they will demand

to be connected to a high-speed backbone. In addition, the tools that are used in the office should be accessible from home or be portable devices that can move from location to location.

Home systems

The heating and cooling systems will be much more complex and energy efficient than they are today. Each room can be set to the preferred temperature and humidity of the occupant. The house will be heated only when necessary because the car will notify the house when an occupant enters the neighborhood. Not only will the garage door be opened and the lights will be turned on, the correct temperature can be set. A connection can also be established between the home heating and cooling system to the power provider. The power provider can notify the home when the most cost efficient time to utilize the power, and the heating and cooling cycle can run in conjunction with the best times.

Home security systems will not be that much different from what we have available today. The use of retinal scans and voice verification may eventually do away with the conventional lock and key, but it will be a long, long time. The newer systems may be able to identify who is home and send a message to the other members of the household. Or the system may be able to use cameras to identify a prowler or someone who shouldn't be there. Smoke detectors will be able to alert the family members no matter whether they are in their bed or on their way home.

New advances in healthcare services in the home may greatly benefit some people. Checking the doctor's schedule with the household schedule would make

setting up appointments easy. Medications can be monitored and health records can be easily accessed. For a person who has diet restrictions their consumption can be carefully monitored. The refrigerator will know who is taking which items, and whether or not they should be. It may be able to track calorie consumption, or make notes to diabetics (Kaye, 1997). Remote checks can be done with elderly people instead of requiring an in home visit. This could be made possible by installing cameras that are only activated if a problem is detected (Harris, 1998).

Maintenance will be much easier as well, because the devices will know when they are not functioning properly. For example, the washing machine could diagnosis itself, go to www.maytag.com, download the necessary software or alert the Maytag repair man that service is needed (Poor, 1997). The systems in homes will need to be as maintenance free as possible. They should automatically download and install upgrades, and prevent viruses from infiltrating the system.

There are some believe that this home of the future will never exist. Having a razor that is IP-enabled is ridiculous, and cost prohibitive (Talley, 1998). Whether or not this home of the future is a reality is not the issue- the issue is that with this example alone there are approximately 45 devices that need to be networked, tracked and on-line. This reaches far beyond the 3 or 4 devices that are currently part of the current onset of technology in the home. The value of having a device that is computer enabled is a good thing. The value of having a device that is computer enabled and networked is a great thing (Huffstutter, 1998)

Homes within communities

Each home will be part of a larger community. The community may be as small as a township, or as large as a city or state. There will be a connection between the home and the work environments. People will need to electronically communicate with the town hall, the post office and the local schools. Retail merchants will develop new kinds of relationships with their customers. Very few internally "connected" or "wired" homes will be isolated from all outside entities. It will be important for homes to be able to access information whether it is around the corner or on the other side of the world.

Within a neighborhood or city there will information that can be shared and accessed frequently. This information would include the community schedule, the doctor's and hairstylists, and the local schools. Homework could be downloaded, and grade reports could be emailed (Thomas, 1998). The grocery store would also be connected to provide a seamless connection between the refrigerator and the food that resides in it. It can also provide information about the baby sitters availability and what experience they have.

This trend has already been witnessed by the growing dependence people have on the World Wide Web. Stocks are tracked, weather is monitored, and in some cases parents can watch their children at a local daycare with real time video. Most of this is accomplished by using web browser located on a PC. Eventually an individual device or a system will be able to track this information independently. Instead of one PC doing all of the communication, it will be several devices seeking out separate data.

Home networking scenario

In order to further simplify the examples it will be necessary to create a base line scenario of what the average home will contain and how it will function. Some of the assumptions are as follows:

1. Control center- service gateway.
There will be single server that will control the major functions within the system. This server may be bypassed if needed. The gateway will be able to manage updates, perform some switching functions, maintain personal databases, and act as a firewall, but it will not be the only access point for the entire system.

2. Service providers
This control center will be directly connected to a single service provider that maintains the unit, so that the homeowner is not directly involved in this process. Each home can have more than one service provider.

3. Direct connection
Some devices will have the ability to directly connect with the outside network and will not require going through the gateway. This group of devices will be made up of traffic, weather and news monitors, books and appliances that will be need to have frequent communications, such as the refrigerator and the gaming center.

4. Isolated devices
Objects such as the remote controls, sensor controls, alarm clocks and artwork will not have the ability to directly access networks beyond the RAN (Residential Area Network). This type of traffic can be controlled by the gateway. This will cut down on non-critical applications from interfering with the other higher priority communications.

5. Fiber
Fiber to the curb or other broadband connections will have to be a part of the system in order for the home environment to be somewhat ubiquitous. Fiber would be the primary source of bandwidth for data intensive applications.

6. Wireless
Almost all of the devices inside the home will be wireless, and there will be receivers and transmitters placed throughout the home to pick up and transfer the signals. The devices that require large amounts of data and are stationary may remain wireline, taking advantage of the fiber to the curb.

The one common thread throughout the home network is at the most fundamental level- how the packets will travel from one node to another and from one

node to the rest of the world. In this particular scenario, the Internet will play a large role in the future. Not only will the devices be communicating with each other; they also will be communicating with their neighbors, the community and the rest of the world.

Bill Gates predicts that Americans will be living a web lifestyle by the end of the first decade of the new millennium (Greenberg, 1997). Web lifestyles means that browsers will be responsible for tracking the household inventory and sending the data to the grocery store. The web browsers of tomorrow will probably not resemble what they look like today, but the bottom line is that the backbone of the Internet, the largest network in the world, is the Internet Protocol. How will the new version fit into the latest generation of networks, the Residential Area Network? Will it be able to handle the types of communications that will be necessary?

Workflows and Data Exchange

As homes progress towards down this path of smart appliances and computer embedded devices there will be requirements that must be met in order for the system to create a ubiquitous computing environment. Although many of these needs are similar to other networks, there will be specific components that are much more important than in any other environment. The average consumer will not be able to deal with problems that require a full time staff. There are many issues that need to be addressed and confronted before the future of the home becomes a reality.

The system must be able to handle multiple devices with individual identities. To have intelligent devices they must know what and where they are (Hawley, 1996). A universal identity system will allow objects in a particular place or in a particular circumstance can behave in a specific way. In places where there are one or two

computers today, there will be a hundred computers and the same amount of connections required. The network will need to possess the ability to interconnect "everyday objects" (Poor, 1997). The density of connections will dramatically increase beyond the capacity needed today. It will no longer be the lone PC requiring only a single connection to the Internet. It will be ten or twenty devices that will be frequently exchanging data.

The home networks will need to handle an extremely high density of nodes. In the average room there may be 10-15 devices interacting with each other. In addition, one or two of these nodes will need an external connection to another network- more than likely the Internet. Because these systems will be highly personalized, there will also need to be a database to store each individual's preferences and schedules. This database might simply reside in a single appliance and then can be shared with the other devices as they enter into the environment. Data will constantly need to be gathered and updated throughout the entire system. The workflows need to be able to handle changes in peoples' moods, and changes in how they like things done.

There will be a consistent exchange of information. As an example, a person comes home from being at work all day. The telephone system will need to switch from the external network to the internal network. The Personal Digital Assistant will transfer the latest updates from the changes in the schedule and maybe other pieces of information that were decided on during the day. At one point the user may have decided what programming they wanted to watch that evening and it is downloaded from the PDA to the home system so that the entire program could be downloaded. The PDA could also notify the home system what type of mood the person is in, and that

information could be used to determine the lighting conditions and the music; maybe even the artwork.

As the person moves through the house, the lights will be turned on, and the temperature conditions could be modified. The news and weather reports could be updated just as the person is approaching the device that is used to keep that information. Not only does the system need to track where the person is in relation to the device; it may need to download the current data. This will be especially complicated if there are several people in the home at one time. People will be constantly moving from room to room and creating different demands wherever they go. If two people are present in one room, the device must attempt to accommodate all of the people present.

There are two basic types of data transfers within the home. Sense and control devices and data transfers. The sense and control components will be primarily connectionless and asynchronous. This type of activity and information exchange is small pieces of data that are sent infrequently. These communication links must be reliable because the user will immediately notice whether or not the system is responding to the environment or commands (Residential, 1999). The thermostat system is a perfect example of this type of data flow. A sensor located at the doorway would receive a signal that a person has entered the room, much like the motion sensors that are being used today. The system may be slightly more complex because it may be able to recognize the occupant. Once the initial signal has been received, another transmission can be sent to the server or command unit. The command unit, which may store the preference database, would then send a signal to the heating and cooling system that would be activated until the appropriate temperature was achieved. These

commands are simple, small and repeatable. They are also asynchronous and isolated to the boundaries of the structure.

Data transfers will have a different list of requirements. These types of transmissions will need to handle both asynchronous and isochronous data transfers. In many applications such as multimedia or entertainment, there is a potential for long data streams which would require simultaneous channels (Residential, 1999). The future television will require two-way communication, input and output. Unlike the TV sets of today, the user will be able to program in the content that will be viewed. The shows will be downloaded from the service provider, or they will be broadcast as they are today, and the receiver picks up the transmission. The ability to rewind pause or fast forward will be available. In order to handle this type of data transfer it will be necessary to have a streaming data path and a secondary smaller communications channel.

These larger bandwidth requirements cannot prevent the flow of other data from coming in or leaving the house. The telephone cannot temporarily be put on hold, and the gaming center can't wait for a large TV download. The network has to be able to handle simultaneous commands and process many different kinds of data simultaneously. One type of transaction must be independent of the other activities that are going on. A bottleneck would not be acceptable in this type of environment. The data transfers will need to be isolated from the sense and control data, so that one will not impact the others' performance.

Another aspect of data transfers is the ability to add a new device into the environment. As a device is implemented into the home, it will need to be able to figure

out all of information of where it is in the network and what the other devices are in the general vicinity. When something is activated for the first time it will need to be programmed to discover important information so that it can be integrated. This will require several messages to be generated, delivered and verified. It is important that every device has some sort of security measures that will be a component of all of the workflows. Some part of the system needs to address the ability to modify the workflow as the environment changes and evolves.

Reliability

It is crucial reliability is built into the installed systems. If the system isn't reliable it will not be acceptable. The network cannot have problems with interference, noise or delay. When moving from room to room it will be critical the network can handle these types of transitions. When moving from inside of the house to the outside environment it will also be necessary to ensure the transitions are seamless.

Most components cannot afford downtime, especially appliances like the refrigerator. The mean time between failures must be minimal because people will not accept flaws in the systems. If a single transmission is dropped or lost it will not greatly affect the entire system, but the system, as a whole should be very robust. More complex connections mean the system will be more fragile. There are several ways to increase the robustness. Only supporting the necessary services minimizes risks, adding anything extraneous could affect the primary service. Devices must be able to self diagnose and authenticate and have a design with fault tolerances. In addition, the system should have the scalability and avoid mechanism that can cascade failures (Oosthoek, 1997).

IP is a best effort delivery mechanism, which means that IP will not guarantee that it will handle the problems of datagram duplication, delayed, out of order, loss of packets or corruption of the data. IP is designed to handle these problems and relies on Transmission Control Protocol (TCP) to provide reliability to the TCP/IP protocol suite (Comer, 1997). TCP is the transport protocol that provides flow-control, full-duplex communications and stream interface. It is the combination of TCP and IP that gives IP the fundamental reliability that is necessary for most applications.

Interoperability

One of the advantages of the Internet Protocol is how prevalent it is in networking the world. The user must not perceive that they are using different networks. Traditionally voice communications have been associated with connection oriented switching technologies. However, there are many companies pushing for a purely IP based solution that will facilitate all types of communications, including voice. Voice over IP (VoIP) has been deemed the ultimate solution for inexpensive voice communication. When IP carries voice, it may become the dominant protocol across all applications. In order to have the Quality of Service (QoS) traditionally associated with switching technologies there will have to be improvements in the upper layer protocols to support a highly reliable IP

The systems implemented into a residential area network must be based on an open architecture. All of the components must be able to interoperate with objects of the same kind and other components in the rest of the system. This can be accomplished by having separate sub systems that communicate within a group of defined objects and

then require another interface to communicate with the rest of the system, or each and every object can communicate with every other component (Residential, 1999)

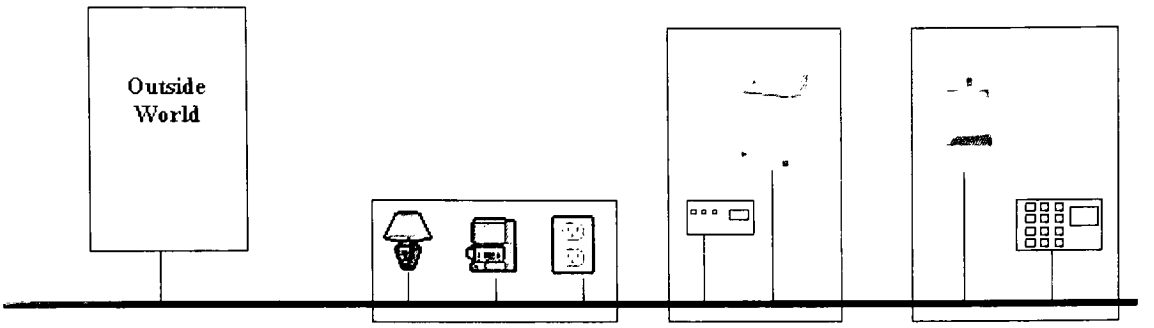


Figure 1 (Residential, 1999)

This may be accomplished by using several different protocols or the use of cross platform applications. IPv6 will not stand-alone, just as IPv4 does not. Many upper layer protocols will provide more features and capabilities than IP alone. One such protocol is the Sun Microsystems Jini connection technology. Jini technology is a platform-independent language based technology built on the Java platform. The technology uses the existing infrastructure of the network so older devices can remain viable along with the Jini enabled devices. In other words, IP would still be the primary network transport, while Jini gives the device the ability to be truly ubiquitous.

The Jini technology has four parts that are designed to make connectivity simple and ubiquitous. A device using Jini will be capable of a feature known as "instant on" The device will be keep its status on the network up to date, and will be automatically ready to interact with the rest of the network with no assistance from the user. The device can also be a part of an Impromptu community without having to make

administrate changes. In addition, Jini allows for devices to be resilient in situations where other parts of the networks fail (Sun, 1999).

There are four layers of Jini- Directory Service, JavaSpace, Remote Method Invocation (RMI) and Boot, Join and Discover Protocol. When a device is plugged into the Jini network, it is immediately registered by the Directory Service layer as a member of the network. The data about the device is placed in the JavaSpace layer so other nodes can discover and download them when interaction is needed. The actual communication with objects in JavaSpace is done using the Remote Method Invocation (RMI) interface and layer. All of the components are announced and registered through the boot, join, and discover layer.

With new technologies such as Jini being frequently announced it is easy to envision a world where devices will be able to function in seamless environment. IP can remain the dominant lower layer protocol, while other protocols above it can enhance the features that IP already has incorporated. IP will continue to coexist with many other protocols, and that will be an attribute that will keep it viable well into the future.

Internet Protocol version 6 vs. Internet Protocol version 4

Introduction

The Internet Protocol is an ideal solution for the needs and demands of data flows and exchanges needed inside and outside the home. IP has the ability to manage the interaction of devices within the network and out to the Internet. It has the flexibility to cross all platforms and connect systems throughout the world. It can handle

asynchronous data and isochronous data such as Voice over IP IP will be an important part of the home networks in the future. Although IP has proven to be an extremely successful protocol, there can always be improvements to performance. Performance can be improved by making modifications to the maximum transmission unit size and maximum packet size, as well as design of the headers and the ability to seamlessly add new options in the future (Loshin, 1999).

There are four main areas of home networking that are the most important- the increased volume and high density of devices, security, ease of use and data flow. These four features are critical for the home-networking environment. These features are also important in the commercial environment, but there are other means of handling them. For example it is not uncommon for a corporation to have a full time staff managing the systems. The staff has the expertise and resources to configure the networks, keep the system up to date and find the latest security solutions. The average homeowner does not have this type of capability. In some cases the demands on a home network are much higher than in a business environment.

At the current time home networking doesn't exist on a large scale. The number of homes with computers is on the rise, but the average home only has one computer. There is no doubt that the number of devices will greatly increase as home networks come on line. Eventually, the average on-line home will contain about 45 devices. Not all of these devices will have the ability to directly connect to the Internet, but it is likely that the combination of commercial sector demands and the home networking demands will outstrip the capability of Internet Protocol version 4. Not only will this be an

addressing issue; it will be an issue of effectively routing the explosion in traffic and the expansion of the number of routers that will be necessary.

As previously discussed in the homes in the future section, the sensitivity and privacy issues will be a great concern for every homeowner. Security will have to be fail-safe. It is critically important that privacy is protected at every level. In some cases the manufacturer will have total access to all of the activity, usage levels, running conditions, repair records (Merloni, 1999). This means that the owner is vulnerable to abuse and misuse of the information that is collected and stored. An intruder cannot have the ability to penetrate the system or monitor the activity from outside the home. The data must be isolated for use in the home and very controlled release of information to the authorized companies. Security violations could potentially put many people at risk.

As Rod Schrock of Compaq Computer Corporation stated- "most households don't have an system administrator, a successful home networking specification has to be simple, foolproof, and inexpensive" (Electronics, 1998). Most people don't program the clock in their VCR. The last thing a consumer will want to do is enter in 75 digits and figure out the server ID and host ID. "Configure" is not a word that majorities of people like to hear. The average consumer does not possess the ability to program their new toaster or rewire an entire network configuration. IP must be able to seamlessly integrate new devices or have the ability to work with other protocols at other layers. Ease of use has to achieve a level of ubiquity.

Data flow is another important component. The amount of data that will flow in and out of the homes will greatly increase. There are many applications such as

video conferencing, multimedia and other forms of entertainment that will require not only large amounts of bandwidth, but also the ability to stream data without delays. All of the information systems will need to be accessed by multiple users. Traffic reports, weather reports, music, video, community calendars, school calendars, appointments, grocery transactions, office and business reports and shopping will all weigh heavily on the systems. Children will demand 3-D and high-resolution imaging. Colors, sounds and images will need to pump through the wires at an astounding rate.

These needs are not new to networking environments. Every day there are improvements and drafts being created to overcome these obstacles with the current version of IP Classless Internet Domain Routing and Network Address Translation have been created to address the issue of the address space and routing issues. Firewalls and authentication have been implemented to address security issues and there are many types of autoconfiguration that have been developed. Data flow has been viewed from every angle- from the physical layer to tags on each header. Can we continue to create innovative solutions on the IPv4 platform, or is it necessary to take it to the next step with IPv6?

Volume issues

The Internet has been growing at an astounding rate since its inception. In 1991 there were three dangers that were created due to the rapid growth of the Internet, exhaustion of the class B addresses, routing table explosion and address depletion (Huitema, 1995). If the Internet Assigned Numbers Authority (IANA) had continued to allocate addresses in the same manner, all of the addresses would have been assigned by the mid- 1990's. Fortunately, solutions were created to deal with these problems.

Few people realized the Internets' potential. It continues to have exponential growth and needs and demands are added every day. Figure 2 shows the growth that the Internet has experienced in the last 8 years.

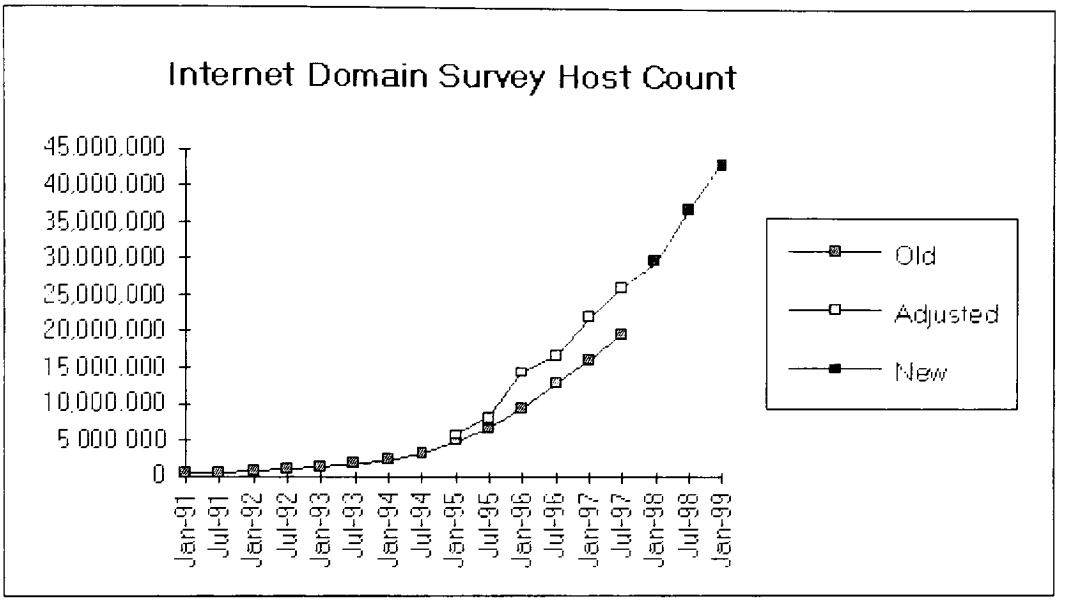


Figure 2 (Number, 1999)

IPv4 Addressing

Each host must have a unique IP address in order to send messages in the global network. The IP addressing scheme allows for different hardware to become a part of dissimilar networks. The current addresses are 32-bits; four fields of one byte (8-bits) divide each. There are three parts to an IPv4 address- a network, a subnet and a host. These network numbers and host numbers are broken down into three primary IP address classes and two special classes.

Class A addresses use the first byte for the network number and the last three bytes for the host numbers. This class can have 128 networks and up to 16, 777,216 hosts per network. The class B addresses use the first two bytes for the network number and the last two bytes for the host addresses. There are a total of 16, 384 networks with 65, 536 hosts per network for this class. Class C uses the first three bytes for the network numbers and the last byte for the host number. This allows for 2,097,152 networks and about 256 host per network. There are approximately 4.2 billion possible combinations of IP Addresses (Goncalves, 1998). At any one point in time 4.2 billion hosts can be accessing the Internet. Even though the current 32 bit IPv4 address structure can enumerate over 4 billion hosts on as many as 16.7 million networks, the actual address assignment efficiency is far less than that, even on a theoretical basis (Huitema, 1994). This inefficiency is exacerbated by the granularity of assignments using Class A, B and C addresses. [RFC 1752] (Request, 1995).

IPv4- Address Types

In addition to network addresses there are directed broadcast addresses, limited broadcast addresses and loopback addresses. The class D addresses have also been set aside for multicast addresses. The range of addresses is from 224.0.0.0 to 239.255.255.255. The directed broadcast address is used to deliver a copy of a packet to all hosts on a physical network. This is achieved by sending the message to a network prefix with a suffix of all ones. This address is not assigned to a specific computer, but is picked up by every node on the network. If the network is not local a single packet is sent across the Internet and the packet is copied and delivered to all of the hosts.

A limited broadcast address is only delivered to a local physical network. It is only sent to the nodes that are on a single wire. This type of address is made up of all ones. There is also a "this computer address" that is used on boot up for the computer to obtain its IP address. This address consists of all zeros. There is also a loop back address that is used for testing network applications. The network prefix of 127 is set aside for loopback addresses.

IPv6 Addressing

When IPv6 was designed, the designers decided to make the leap to 128-bit addresses, which means 340,282,366,920,938,463, 463,374,607.431,768,211,456 addresses are possible. This expansion of addresses will accommodate the future growth expected. This is equivalent to about 32 addresses per square inch of day land on the entire earth's surface (Miller, 1998).

There are three different forms for representing IPv6 as text strings.

1. x:x:x:x:x:x:x:x
Where the x's are hexadecimal values of eight 16-bit pieces of the address. In this form it is not necessary to write the leading zeros in an individual field, but there must be at least one numeral in every field.

2. x:x:x:x::x:x:x
Where "::" can be used to signify multiple groups of 16-bit zeros. The "::" can also be used to compress the leading and/or trailing zeros in an address.

3. x:x:x:x:x:x:d.d.d.d
This is a used in a mixed environment where IPv4 and IPv6 nodes exist. The x's are the hexadecimal values of the six high-order 16-bit pieces of the address, and the d's are the decimal values of the four low-order 8-bit pieces of the address.
[RFC 2373] (Request, 1998).

There are also address prefixes in IPv6 and is noted similar to CIDR in IPv4. The notation represents it: IPv6-address/prefix-length. The prefix length is a decimal value specifying how many of the leftmost bits of the address make up the prefix. The

leading bits in the address indicate the specific type of IPv6 address. The variable-length field comprising these leading bits is called the Format Prefix (FP). The initial allocation of these prefixes is as follows:

Allocation	Prefix	Fraction of (binary) Address Space
Reserved	0000 0000	1/256
Unassigned	0000 0001	1/256
Reserved for NSAP Allocation	0000 001	1/128
Reserved for IPX Allocation	0000 010	1/128
Unassigned	0000 011	1/128
Unassigned	0000 1	1/32
Unassigned	0001	1/16
Global Unicast Addresses	001	1/8
Unassigned	010	1/8
Unassigned	011	1/8
Unassigned	100	1/8
Unassigned	101	1/8
Unassigned	110	1/8
Unassigned	1110	1/16
Unassigned	1111 0	1/32
Unassigned	1111 10	1/64
Unassigned	1111 110	1/128
Unassigned	1111 1110 0	1/512
Link-Local Unicast Addresses	1111 1110 10	1/1024
Site-Local Unicast Addresses	1111 1110 11	1/1024
Multicast Addresses	1111 1111	1/256

Table 1

Fifteen percent of the address space is initially allocated, with the remaining unassigned addresses reserved for expansion of the existing use or new uses such as separate locators and identifiers. Anycast addresses are taken from the unicast address space and are indistinguishable from each other. Multicast addresses have a value of FF (11111111) in the high-order octet of the addresses.

IPv6- Address Types

There are three types of addresses in IPv6 addressing- unicast, anycast, and multicast. Broadcast addresses have been replaced by multicast addresses in IPv6.

The IPv6 addresses are assigned to interfaces not nodes. Each interface relates to a single node, but there can be several interfaces associated with the same node. Each interface can have more than one type of address (unicast, anycast or multicast), but it must have at least one link-local unicast address. There are still several special addresses, such as unspecified addresses, which is used during startup if a node doesn't know it's own address and the loopback address, which is used to send a datagram back to itself. There are also IPv6 addresses that contain an embedded IPv4 address.

There is one main difference when relating IPv6 to the IPv4 addressing scheme. In a point-to-point link in an IPv4 network it is necessary to have an IP address for all the network interfaces in the transmission, including routers. In IPv6 there is some efficiency with point-to-point transmissions if the link is not originating or receiving IPv6 packets. It isn't necessary for all of the interfaces to have specific IP addresses, thus saving address space. If two nodes are merely passing traffic they do not need to have IPv6 addresses (Loshin, 1999).

Unicast

There are several forms of unicast addresses: aggregatable global unicast address, NSAP (Network Service Access Point) address, IPX (Internetwork Packet eXchange- Novell NetWare) hierarchical address, the site-local address, the link-local address and the IPv4 capable address. Unicast addresses are designed assuming that the routing decisions are based on a "longest prefix match" [RFC 2374] (Request, 1998). The node can be made aware of as much or as little of the address as needed, depending on the node's function. The address may be viewed as a single piece of

information or the information can be parsed into smaller pieces (Loshin, 1999). In the end, the address still needs to be 128-bits, and will identify a nodes interface.

The unicast address is designed to support current provider aggregation and a new type of aggregation called exchanges. Provider-based aggregation means the addresses would be assigned based on the service provider. Large organizations with several service providers would have difficulty managing different address. Changing a service provider would require reallocation of addresses. The geographic based option was considered, but then dismissed. The option selected was exchange-based addresses. These addresses are allocated through the Internet provider. An address block is assigned to a service provider and the subscriber accesses the network through the provider. There is little maintenance required on behalf of the subscriber (Loshin, 1999).

There are 5 parts of a unicast address. The first part is the 3-bit prefix 010, which is then followed by the Top Level Aggregator (TLA). The TLA can either be a provider or an exchange point. The routing tables will only need to have one entry per TLA. The TLA's are 13-bits, which means there can be 8,192 exchange points or backbone providers (Huitema, 1998). There are 8-bits reserved between the TLA and the next frame. The next address component is the Next Level Aggregator (NLA) which is 32-bits long and will be used to allow the ISP's to implement their own addressing hierarchy. The site-level aggregation identifier is given to organizations for their internal network structure and is 16-bits long. This portion of the address supports 65,535 individual subnets per site [RFC 2374] (Request, 1998). This should be sufficient for all but the largest organizations. The last field in the address is the interface identifier.

A unicast address may be viewed as a two-field entity, one identifies the network and the other identifies the nodes interface. The interface identifiers are required as part of the addressing architecture, and are based on the IEEE EUI-64. This is a 64-bit identifier is used to uniquely identify each and every network interface, which means that there can be 18 billion billion different addresses, which is only half of the IPv6 addressing space.

There are three levels of the hierarchy: public topology, site topology and interface identifier. The public topology is the public Internet transit services. This is the global part of the network that requires unique global addresses. As with the Network Address Translation (NAT) used in IPv4, there may be certain circumstances that do not require addresses to go beyond the scope of the organization. There have been two different segments of the address space allocated to support this ability (Loshin, 1998). There are two types of local-use unicast addresses: link-local and site-local. Link-local addresses are used in auto-address configuration, neighbor discovery, or when there are not any routers present. These addresses are intended to identify hosts on a single network link. Site-local addresses are used internally within the site network, and cannot be used in the global network. Routers will not forward packets with site-local or link-local source addresses (Miller, 1998).

The design choices for the size of the fields were made for several reasons. One of the reasons is to insure that the default-free routing tables are manageable in size and the amount of examination that needs to be handled as the internet grows in complexity and size. As an example, the controls that monitor the location of the participants would

have a site local address that is not used in the global network. There is no need to distribute this information to any other location. Unique global addresses are not needed and it would not be necessary to advertise the address outside of the local network. The site local address would only be used for communication between the location and a primary control center. Not every device will need to have access to the Internet. Keeping a device isolated within its own network will minimize the impact of resources on the global network.

Anycast

Anycast addresses are a single address assigned to more than one interface and are designed so only a single node will receive the datagram, usually the closest node. For example, if a request is sent out to get the time from a timeserver, the message will be addressed to any router that has an associated timeserver. However, it is most effective if the closest available timeserver responds. Once the datagram reaches the closest timeserver, the node will respond and the original datagram will not travel any further. This is helpful for certain types of services that do not require a relationship between the client and the server (Loshin, 1999). The other uses for anycast are identifying a set of routers that belongs to an Internet Service Provider, a set of routers that are part of a particular subnet, and a set of routers that provide an entry to a particular routing domain (Miller, 1998).

Part of the anycast address is a prefix that identifies the topological region in which all the interfaces reside. Within the region each member must be advertised as a separate entity, and outside of the region it will be identified by its prefix. If the members were not located in one region it is possible that all of the addresses would be advertised to the entire Internet. It is necessary to severely limit the use of anycast addresses

because there is a potential for an explosion of messages. There are currently two limitations placed on anycast addresses. First, an anycast address cannot be used as a source address and second, an anycast address can only be assigned to a router [RFC 2373] (Request, 1998).

IPv6 Multicasting

With multicast each transaction is only carried over each link once. The transmission is "dropped off" and duplicated at each node. This can lead to great improvements in efficiencies over distributed networks. In addition, unlike point to point communications, multicasting is easily scalable (Oosthoek, 1997). The network does not feel the brunt of an increase in traffic, even if the number of recipients is greatly increased. Multicasting achieves this by having three basic requirements: 1) Routers must be able to efficiently locate routes to many networks at once 2) Only a single copy of each packet should be sent on any shared link and 3) Traffic should only be sent on links that have at least one recipient (O'reilly).

There are many uses for multicasting. The need for multicasting continues to grow as the number of users' increase and new applications are more feasible. Multicasting can add significant functionality without impacting the network (Quinn, 1998). This is critical in home-networking environments as uses become more clearly defined because new applications will arise. There are three general categories for multicast applications: 1) One-to-Many (single source to multiple receivers), 2) Many-to-One (multiple sources to one receiver) and 3) Many-to-Many (any number of hosts sending to the same multicast group address and receiving from it). (Quinn, 1998).

An organization called Mbone was established to implement and test multicasting in the early 1990's. Mbone is an overlay network that has been used to accelerate the early usage of multicasting through the Internet (Huitema, 1995). IPv4 has a designated range of addresses that have been identified for multicast. Although a Class of addresses have been identified, a majority of IPv4 routers are not multicast enabled. This requires a multicast enabled router at the source and the destination. Tunneling is used to forward multicast packets throughout the rest of the network (Whatis.com). The Mbone solution does not fully capitalize on the efficiencies and capabilities of a truly multicast enabled network. The packets must be encapsulated and assigned a unicast address while traversing the non-multicast enable portion of the network. There are many constraints on IPv4 multicasting, such as limited processing capabilities, risks of local congestion, and disruption of non-multicast traffic. Although many issues have been identified and resolved through Mbone, it is not intended for full-scale implementation of multicasting throughout the network.

The designers of IPv6 wanted to ensure that all IPv6 nodes could take advantage of multicasting. The multicast addressing that is used in IPv6 can be identified by all routers and all of the experience that has been gained in Mbone's IPv4 multicasting has been incorporated into IPv6 multicasting. Multicasting has been part of the development of IPv6 since the beginning, so in a fully deployed IPv6 network multicasting is a seamless and advantageous. Please refer to the Multicast section on page 35 for further discussion of Multicasting.

Address Depletion

At the current time there are approximately 100 million households in the United States, 24 million households in Great Britain (Office, 1998) and a total European population of approximately 735 million people (Global, 1998). One-fifth of the world population lives in a developed nation and the European and U.S. markets will probably be the first to adopt home networks. With an estimated 200 million households in Europe and the United States it is probable only 40% to 50% will adopt the technology. There will be approximately 100 million networked homes at some point in time in the future. If each home has 20 devices there will be a total of 2 billion devices. At most there will be 40 devices in each home for a total of 4 billion devices. With an average of 2-4 billion devices only a small portion of these devices will be active in the global network at any given point in time. It is possible that each home will only need 4-6 IP addresses because of the gateway's ability to manage the traffic leaving the home. This means that a minimum of 600 million addresses will be necessary for home networks. This does not include the devices that will be needed in the commercial sector, which has already taken half of the current address space.

The current world population is approximately 6 billion people with a projected 9 billion people by the year 2050 (United, 1998). Approximately 1-2 billion people will live in developed nations. Each person will need a minimum of one address for home and one address for work. A minimum of 4 billion IP addresses will be needed. IPv4 can only support 4.2 billion devices accessing the global network at one point in time. In the early 1990's the Internet Engineering Task Force was faced with making a decision based on the prediction that the current IP address space would be exhausted in March of 1994 (Miller, 1998). With approximately half of the 4.2 billion IPv4 addresses already

assigned, it is estimated that the address space will run out by the year 2010. Some experts suggest that IPv4, with its IPv6-like feature enhancements, will suffice for more than a decade. Smarter ways of handling router tables and creatively using Network Address Translation (NAT) in IPv4 might meet the demands of the commercial and home sectors well into the 21st Century. Others predict that the emergence of technologies and devices will require every individual on the planet to have an IP address will drive the need for IPv6's expanded addressing scheme much sooner (McNealis, 1998). IPv6 will eventually need to replace IPv4.

IPv6 does not have the limitations of IPv4. There are enough unique addresses available in IPv6 to sustain the expected growth of smart appliances and devices well into the next century. With 128-bit addressing there are 340,282,366,920,938,463,463, 374,607, 431,768,211,456 possible addresses. This expansion of addresses will accommodate the future growth expected. There can be approximately 32 addresses per square inch of day land on the entire earth's surface (Miller, 1998), which is more than sufficient for ubiquitous computing.

Network Address Translation

Network Address Translation is a way to prevent the depletion of addresses with IPv4. It does this by translating the IP address used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. (Whatis, 1999). The local network addresses are mapped to one or more global outside addresses when sending a packet from inside the network to the outside. When an outside packet is sent in the global IP address is mapped to the local IP address. The NAT enabled device maintains a table of inside and outside addresses.

The key to NAT is that local hosts must have a globally unique address while accessing the Internet, but it doesn't mean that the host always has to have access to the global network. The addresses can be reused among the resources in the local network. Only a small percentage of hosts within a sub domain communicate outside their domain at one time (Goncalves, 1998). This would be true of the devices found in the home.

NAT works by maintaining a table of local addresses and IP addresses. The local address doesn't need to be unique because it will be isolated within its own domain. Firewalls or packet filtering routings keeps the network separate from the Internet. The local networks can use the same addresses currently being used in the global network, because the data doesn't effect the external network. When the host needs to go outside of its domain it will "borrow" a legal address that is unique in the global network. A pool of legal addresses is maintained for all of the internal hosts to access as needed. The local network is virtually invisible to the public and there is no need to reconfigure each host if there are changes to the addressing structure.

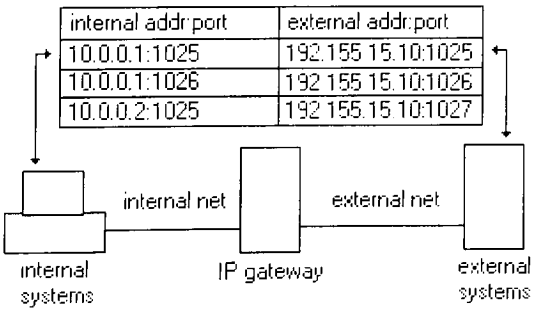


Figure 3 (Hall, 1997)

There are several positive aspects to NAT. The first is that it is provides a firewall type of environment. This means that a node sending a packet into the system will not know the final address of the recipient. In essence this means all of the devices inside the network cannot be detected by outside sources. Changes inside the network will not effect the outside network. The NAT device can also track all of the traffic passed between the two networks.

There are limitations to NAT, especially in environments that heavily depend on the Internet and need constant access. In this scenario, each host should be designated an individual IP address. In addition, a bottleneck can be created at the NAT device that resides at the edge of the network because each and every packet has to have an address substituted. As a result each packet needs to be handled, which slows down the packets' progress. As more and more NAT devices are added to a growing network, it becomes more difficult to synchronize multiple NAT devices within a single enterprise (Goncalves, 1998). In addition, NAT has certain limitations with IPsec, which will be more prevalent as Virtual Private Networks (VPN) are implemented. There are certain configurations and combinations of NAT that will not work with IPsec. With NAT there can only be 4.2 billion devices communicating in the global network at any one given point in time. This might not be able to sustain the amount of activity that will be required in the future.

Although most of the devices within the networking systems are very reliable, there is still a possibility that the packets may be mis-addressed. There are also several types of applications that cannot work in conjunction with NAT. IP multicast, routing table updates, DNS zone transfers, BOOTP, talk and ntalk, SNMP and Netshow are

traffic types and applications that cannot be supported through NAT(Cisco, 1999). The other aspect that is a shortfall of NAT is that it hides the identity of hosts, which can be considered positive from some aspects of security but not from others (Francis, 1994). With NAT anything that carries an IP address cannot be encrypted. This is definitely a weak point for NAT.

In a majority of cases NAT is referred to as a temporary solution to the impending reality of a shortage of addresses. There are too many limitations that restrict NAT from being effective in a home-networking environment. Encryption, IPsec and multicast will be too important to overlook when using NAT.

Class B Addresses

The IPv4 class system makes it difficult to administrate addresses, because there are few organizations that will have as many as 16,777,216 hosts or as little as 256 hosts. Most groups need somewhere in between this number and moving up from a C class to a B class address means the difference of 256 to 65,536 hosts. This can be inefficient and wasteful. CIDR makes the address space more efficient by replacing address classes with address prefixes and network masks. This allows several class C numbers to be allocated instead of one single class B number. It gives the ability for organizations to get only the number of host addresses needed. As an example, if an organization needs 512 addresses, they would be assigned 2 contiguous class C networks. If they need 1024 they would be assigned 3 contiguous class C networks, and so on. CIDR can help better utilize the addresses that exist, and make the administration of these addresses a little bit easier.

The home networks will need to rely on Internet Service Providers, so classes of addresses will not make a difference to the individual homeowner. The biggest issue with the problem of the class structure of IPv4 is that it means that there are thousands of wasted addresses because the assigned class does not meet the needs of the individual organization. It is possible with CIDR that each and every bit of the 32-bit address can be utilized, but it can be very difficult to administrate all of the individual needs. With IPv6 this is not an issue at all because only 15% of all the addresses have even been designated. It would be simple to allocate a small percentage of the addressing space to address these issues.

Routing issues

Routing table explosion is another issue that will continue to be a problem as the number of devices on the Internet grows. Even if there are enough addresses, it is difficult to state whether or not the network could handle this many addresses. With the absence of routing technologies that could scale the size of the Internet to the potential that can be realized with the IPv6 address space, increase in the available address space may not be useful (Cisco, 1999). Potentially, the network may not be able to handle all of the traffic that could be generated with billions of devices. The improvements in the routing schemes of IPv6 should be able to handle this problem, but until it is put into practice it is difficult to prove. Every attempt has been made to ensure that IPv6 will be able to handle the expansion of the Internet, IPv4 on the other hand was not designed for this type of situation.

Each router maintains data about where it resides on the network and its neighbors to effectively and efficiently forward packets. The more information the router maintains the more effective it is at intelligently handling packets, but this creates

inefficiencies. It is impossible for the router to maintain the location or routing path of each node or host. CIDR alleviates some of the pressure on the routing tables by permitting route aggregation at various levels of the hierarchy (Goncalves, 1998), but it doesn't solve the long-term issues. IPv4 has had several means of handling the tremendous explosion of entries on the routing tables, but the system as a whole was not designed to handle a future with every home being connected to the Internet with several devices. There has to be more efficiency than can be currently found in the protocol today.

Table aggregation

Table aggregation can only be achieved by assigning addresses in a coordinated fashion. At the current time there is an aggregation of addresses based on common prefixes that is organized by regional scope. Up until 1992, there was no relation at all to the delegation of network addresses (Huitema, 1995). There was a lot of flexibility, but it also caused an explosion of routing tables.

There are two thoughts about how to approach organizing the IP addresses. The first option is geography. Addresses would be assigned by country or by city. A city is next to B city and C city is next to D city. A problem exists when the Internet Providers are not local. A packet can end up travelling a long distance to reach the ISP and then travel back to reach a neighbor right next door. The Internet is not "organized" in a geographical fashion, which makes it difficult to implement and justify a geographical hierarchy.

The other option is to go with provider addressing. Each Internet provider receives a slice of the address space and then the addresses are allocated to their

customers. As a result all of the customers have the same prefix and can be aggregated as one single entry in the others providers' routing tables (Huitema, 1995). The problem with this scenario is when the customer wishes to move from one service provider to another. If the customer keeps the original address the provider will have to maintain that address as an exception and forward the packets to the new service provider creating a lot of inefficiencies. In this case the customer would be forced to change the address which means overhead on their behalf.

IPv6 already has aggregation as part of the addressing scheme. It is built into the address, and the plan is to go with exchange based addresses. These addresses are allocated directly through the Internet provider. The exchange provides the address block and the subscriber would access the network through the provider. This means there is very little maintenance on behalf of the subscriber. The IPv6 addressing scheme takes it to another level as well. There are top-level aggregation, next-level aggregation, site-level aggregation and an interface identifiers. The routing tables will only need to maintain one level- the top-level aggregation identifier.

With IPv4 CIDR provides for hierarchically allocation of IP addresses and hierarchical routing aggregation. The route aggregation is accomplished by a single route can cover the address space of several old-style network numbers, which means a single route can replace several older routes (Goncalves, 1998). CIDR replaces the class addresses with a generalized network prefix. This prefix is added to the IP address and consists of a mask length. Blocks of addresses can be assigned for networks as small as 32 hosts up to 500,000 hosts (Goncalves, 1998). There are still some areas of the Internet that do not support CIDR.

Another option considered for IPv4 is using the existing 32-bit addressing scheme as a non-globally unique identifier (Loshin,1999). This could be accomplished by dividing the world into different domains and them using the 32-bit addresses in different domains where they are not interconnected. This type of implementation would require a lot of restructuring and would be difficult to implement.

Ease of Use

Ideally a device should enter its' new environment and be available for immediate use. It should be able to Identify itself and broadcast that information to all of the other components. It should establish an address and its place in the network without the owner evening knowing any information was exchanged. The term plug and play means providing power and the device is ready for action. In a truly ubiquitous environment, the device would already know what house it is in, who the owners are, and at least a few of the owner's preferences. It should also have the ability to immediately connect with the Internet or external network to access any other information that is needed to complete installation.

In order to be truly plug and play capable, the device will need to establish a connection to an external and internal network. It will need to assess its environment and the type of communications necessary. In addition, it must be able to find or assign itself a unique identifier within the local network, as well as finding a way to get a unique identifier in the external network.

This also is true for maintenance and updating. Every time the object needs updating it should not require the user to hunt down the information and walk through the updating process. It should happen automatically, with little to no intervention. Repairs should be the same way. The appliance should be able to diagnose itself and get whatever information is readily available. Only if it is in need of personal attention should it communicate this need to the user. There may also be ways to allow temporary access for the service providers or repair people to get into the system (Restivo, 1999). It is very important that the maintenance is non-invasive and secure.

How will these millions upon millions of devices be handled and managed? It has to be better than requiring each and every computer to have an administrator manually assigning a unique address. Imagine a homeowner sitting down and typing in a 128-bit address. It would be nearly impossible to support configuring every single device in a home environment. There has to be some mechanism that allows the devices to be seamlessly integrated into the network. Migration transparency and scaling transparency are a must. If a service provider is changed or added, the protocol should be able to handle the updating and reconfiguring that is necessary as well. Some of the plug and play features of IPv6 are address discovery, network information discovery, automated address changes, support for mobile hosts and dead neighbor detection.

Without the ability for the average consumer to start using something new right away, it will never be successful. IPv6 gives the ability for devices to essentially manage themselves with very little interaction. There will be other components to the human-computer interaction for plug and play to truly exist, but IPv6 will be able to

manage the ability to get connected to the Internet without having to manually configure every part of the network interface. In addition, with the ability to detect a duplication of addresses, neighbor discovery and a combination of stateless and stateful autoconfiguration it will be enough of a beginning to build for the other parts of the system to rely on.

Autoconfiguration

IPv4 autoconfiguration

Right now configuration is a primarily manual process. A new PC is connected to the network, it is assigned an IP address, host name, subnet mask, default router, DNS server address and other types of parameters. Getting connected to an IPv4 network can be very complicated, time-consuming and costly process (Loshin, 1999). It can be complicated because there are several mechanism that are needed to obtain the configuration information, several methods exist for passing the information to the protocol software and there are multiple methods for configuring any given system (Comer, 1997). There are two general classes of configuration information, internal and external. The internal information would be the device itself, and the external information relates to the devices' surroundings.

It used to be that a computer was moved to a location and only need to be configured once until it was removed from the system. Now devices can be mobile and the task becomes much more complicated. This created the need for some type of autoconfiguration. Initially a Bootstrap Protocol was created, but it was not flexible enough. As a result, Dynamic Host Configuration Protocol (DHCP) was created. Nodes in the network query a server for configuration information on boot and then there are

various means of allocating addresses. The DHCP is a stateful configuration, meaning that the DHCP server must maintain the status of different hosts, and that data must be managed. The addresses are leased to the node and eventually will be reassigned. This type of address management is helpful for large organizations. In addition, current operating systems are designed to assist in implementing IP networks.

There are two different mechanisms to support plug and play network connections. The first is the Boot Protocol (BOOTP) and the other is the Dynamic Host Configuration Protocol (DHCP). These are stateful autoconfiguration mechanisms, which means a server is located on the network that maintains status and administrative data (Loshin, 1999). The server is responsible for administrating any changes and maintains the lists of addresses and nodes. This type of configuration requires human intervention. The other option is stateless autoconfiguration, which means there is not a server that obtains this information explicitly. The node is responsible for gathering the data necessary to determine its' correct IP addresses. Stateless and stateful autoconfiguration can co-exist. In a stateless environment once the IP address is determined the node can assess the DHCP server and get any other data that is necessary for network configuration. The downside to a stateless environment is that it is easy to breach the security. Any node that is connected to the network will be assigned an address and access to the network. A combination of stateful and stateless autoconfiguration would alleviate this problem.

IPv6 autoconfiguration

IPv6 incorporates the DHCP protocol, which allows the host to obtain all of the relevant information. It also supports automated address changes, mobile hosts, and dead neighbor detection. Link-local addresses can be determined by using the link-

local prefix and a unique token that will give the node its unique identity. The link-local address is then used to initiate membership in an all nodes multicast group. A solicitation message is sent out if a router advertisement message is not received during one of the regular intervals. The solicitation message will be sent three times to ensure that there isn't a router on the network. If no router responds, then the node will continue to use its link-local address and only communicate with the nodes on the local network. After this address is established the node will send out another message with the address that it was assigned. If another node responds, it will reveal a duplication of addresses by exposing a collision.

Address resolution and neighbor discovery

Address resolution and neighbor discovery are handled differently than IPv4. Neighbor discovery combines the Address Resolution Protocol, the ICMP (Internet Control Message Protocol) Router Discover messages and the ICMP Redirect message found in IPv4. Routers and neighbors will advertise their availability or solicit an advertisement in order to determine if they are available, to verify addresses, and to establish link-layer addresses (Loshin, 1999). Neighbor discovery defines where the node is on the network, and the path that the datagram must travel in order to reach the destination. Nodes also use neighbor discovery to determine the link-layer addresses for nodes that are on attached links and to purge addresses that have become invalid. This allows for nodes to determine which routers are willing to forward packets on their behalf, and which nodes are reachable and which nodes or not. Neighbor discovery also allows for new paths when the current path fails [RFC 1970] (Request, 1996).

Neighbor discovery is made possible by five different ICMP packet types: a pair of router solicitation and router advertisement messages, a pair of neighbor solicitation

and neighbor advertisement messages, and redirect messages [RFC 1970] (Request, 1996). The router solicitation messages are generated when a new interface is enabled, rather than waiting for the next scheduled time. Neighbor solicitation determines the link-layer address of a neighbor, verifies whether or not a neighbor is still reachable and detects duplicate addresses. The link layer address of a neighbor is determined by generating a solicitation message that is sent to the target nodes' solicited node multicast address. The target then sends a unicast neighbor advertisement back to the originator of the message.

Advertisement messages are sent out periodically to advertise node or router presence amongst the various links. The router advertisements are the mechanism that allows routers how to perform the address autoconfiguration. The router can specify either stateful or stateless address configuration. The hop limit and other link parameters are also contained in the router advertisement message. This information can be administered centrally, and then propagated out to all of the associated hosts.

Neighbor unreachability detection is used to determine the inability to successfully deliver packets to the destination. Upper layer protocols provide confirmation of correctly sent data from recent acknowledgement messages. If this information is not available, or hasn't been received, then a unicast neighbor solicitation message is sent to confirm reachability from the next hop. These messages are only generated when a link is actively sending packets. In addition, neighbor unreachability detection allows for mobile nodes to move off the network without causing other links to fail because the change has been detected and the routes can be easily updated. When an address has been changed, a node can send out an unsolicited neighbor

advertisement packet notifying the neighboring nodes that the current address has become invalid. The redirect message is used to inform hosts of better first hops for the destination.

There are a couple of key improvements from IPv4 to IPv6. The first is that router discovery is part of the base protocol set and no additional packet exchange is needed to resolve link-layer address because the router advertisements carry the addresses and prefixes for a link. Router advertisements make address autoconfiguration possible. More multicast addresses are available to handle address resolution and the address resolution process is much more direct without having to affect unnecessary nodes. Redirects contain more data about the first hop, which means fewer messages will be generated. The protocol is more media-independent than ARP because address resolution is at the ICMP layer, and makes IP authentication and security mechanisms possible [RFC 1970] (Request, 1996). There are IPv6 advertisements that would replace common IPv4 advertisements. Some of the advertisements are consolidated and some of the advertisements are more efficient to minimize the impact on the network.

Security

In the home, one of the biggest concerns is security. There are three potential areas that could be violated; the first is the system security at the protocol level. A hacker might try to get access into the transmissions going from the home into the community, attempting to masquerade as an authorized user. It also includes viruses and other issues dealing with the most fundamental processing components in the system. The second is the audio video data and content. This is equivalent to the data

that currently travels over the cable into the TV. The third component is the physical security of the home- the data that maintains all of the data on the activities in the household, from keeping track of the temperature to knowing which person is present in which room. Including any monitoring devices that are used to protect the physical property, the telecom systems, and all of the appliances (Residential, 1999).

There are multiple uses for security in a home environment. Within firewalls, between mobile units and the home and between secure hosts (Huitema, 1998). There also has to be security in place when implementing a new node into the system. With auto-configuration enabled and neighbor discovery, it may be extremely easy for someone to perpetrate the system with little difficulty. In the home, it is not sufficient to assume the security needs to take place just for the transmissions leaving the home, it will be necessary to secure the transmissions inside the home as well. It is the same idea of having a cordless phones intercepted. The systems designed for the homes in the future may leave the occupants much more vulnerable to attacks from the outside.

One of the keys of Internet-level security is that it simplifies the development of secure applications. It will be the baseline for application developers to build on and it will mean that security is available on all operating system platforms. As more data is shared, the more threats there are to networked systems and the higher the likelihood for invasions of privacy and confidentiality. This is critical in the home environment where much of the data is extremely personal. Confidentiality must be maintained and only authorized personnel can access the information collected and stored. When IPv6 was in its infancy, security was a high priority. With the onset of a new protocol, the opportunity presented itself to be able to implement security within the data link layer,

instead of relying on higher level protocols. IP layer security only protects the IP datagrams. IP security is basically transparent to the user, and can create a foundation for other forms of security to be incorporated.

IPSec

IP traffic is susceptible to interception, sniffers, denial of service and spoofing. Interception occurs when the data transmitted from one node to another is taken from an unauthorized third party. A sniffer is a program that monitors and analyzes network traffic, detecting bottlenecks and problems (Whatis, 1999). Some of these sniffers not only analyze traffic; the actual payload data can be read. Denial of service can happen when an authorized user cannot access the network resources. This happens by flooding the host with requests or unnecessarily sending data only to block the flow of other data. Spoofing occurs when a packet is altered to misrepresent the packets' origin. For a long time security was not considered important at the Internet layer (Loshin, 1999). In most circumstances security issues have been handled in higher layers. Spoofing, denial of service, hijacking and interception of connections have raised the level of interest of security in the IETF (Cisco, 1999).

IP Security (IPsec) is security architecture for the Internet Protocol. It is not intended to make the Internet secure, it is intended to make IP secure. IPsec defines security services that can be used at the IP layer for both IPv4 and IPv6 (Loshin, 1999). The goals for IP security are to authenticate, maintain the integrity and the confidentiality of the IP packets. These are three areas that are very important in the home-networking environment. The security services that are a component of IPsec is access control, connectionless integrity, data origin authentication, defense against replay attacks,

encryption and traffic flow confidentiality. All of these functions will be made possible by the use of encapsulating security payload headers and authentication headers (Loshin, 1999).

The Encapsulating Security Payload (ESP) Header is designed to allow IP nodes to send and receive datagrams whose payload is encrypted (Loshin, 1999). Some of its function overlap with the authentication headers, but ESP adds a level of confidentiality by transforming the data. This header is designed to provide confidentiality of datagrams through encryption, authentication of data origin through the use of public key encryption, anti-replay services through the same sequence number mechanism and limited traffic flow confidentiality though the use of security gateways (Loshin, 1999). ESP does allow for attackers to study traffic because it appears to be a regular datagram, the only difference is that the payload is encrypted. Tunneling and security gateways can also be used with ESP.

Security associations rely on the use of keys. Efficient deployment of security will rely on the existence of an efficient key distribution method (Huitema, 1998). The key management procedures determine the security parameter index as well as providing the keys. There are several proposals that are under examination at the current time: Photuris, Simple Key-management for Internet Protocols (SKIP), Internet Security Association and Key Management Protocol (ISAKMP) and manual key distribution. Ideally, in a home environment the user would be unaware of any authentication or encapsulation at the IP layer. There may be a higher level of authentication so that the system is aware of who the user is, and an outsider cannot

crusade as the home owner, which would greatly defeat any security measures put in place at the data link layer

Virtual Private Networks (VPN) are becoming more popular to address some of the security and privacy issues. VPNs allow a virtually private connection in a public network by utilizing encryption, encapsulation and tunneling. A tunnel mode can be established by two systems setting up a secure association. Once the secure association has been obtained, data can be sent freely between the two systems. Private lines have traditionally been used in situations where security was important. However, private lines are much more expensive than using the public network. VPNs offer a lower cost secure option. IPsec is an integral part of a VPN solution. VPNs may be an excellent solution for a secure inexpensive connection from the home to the bank, where security is an extremely high priority.

IPv4 security is addressed through the use of VPNs, firewalls, IPsec and NAT. A combination of these hardware and software solutions has made IPv4 much less prone to attacks. There are other components that have been added to IPv6 such as the authentication header. The authentication header can carry content verification data for the IP datagram, can create a link to an entity, can provide non-repudiation, and can protect against replay attacks (Goncalves, 1998). It provides explicit insurance for the origin of the data and does not transform the data in any way. (Huitema, 1998). The authentication headers can be used to handle simple datagram transfers, or encapsulate an entire stream of datagrams. The use of the authentication header will prevent hackers from stealing addresses, and therefore intercepting data transmission and stealing connections (Huitema, 1998).

When IPv6 packets are sent they all convey a Security Parameter Index (SPI). Each node must know the SPI to determine the security context, whether it is one node or a group of nodes in a multicast environment. Both authentication and encryption are based on a concept of security association (Huitema, 1998). A Security Association normally includes the parameters listed below, but might include additional parameters as well:

- Authentication algorithm and algorithm mode being used with the IP Authentication Header
- Key(s) used with the authentication algorithm in use with the Authentication Header.
- Encryption algorithm, algorithm mode, and transform being used with the IP Encapsulating Security Payload.
- Key(s) used with the encryption algorithm in use with the Encapsulating Security Payload.
- Presence/absence and size of a cryptographic synchronization or initialization vector field for the encryption algorithm.
- Authentication algorithm and mode used with the ESP transform.
- Authentication key(s) used with the authentication algorithm that is part of the ESP transform (if any).
- Lifetime of the key or time when key change should occur.
- Lifetime of this Security Association.

- Source Address(es) of the Security Association, might be a wildcard address if more than one sending system shares the same Security Association with the destination.
- Sensitivity level (for example, Secret or Unclassified) of the protected data. [RFC 1825] (Request, 1995)

Data Flow

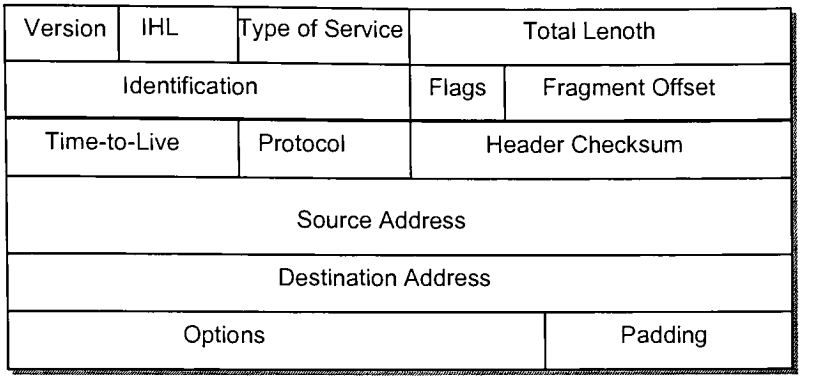
Bandwidth on demand and the ability to control the flow of packets will be important issues. There will be a need for a constant flow of data in and out of the home, which will require steady bandwidth. There will also be a need for data transmissions that are bursty and sporadic. In addition, there will voice which is

relatively low in bandwidth but needs continuous streaming. Whether it is streaming, bursty or real-time, IP is poised to be one protocol that will be able to handle all types of communications. Bandwidth will need to continually increase as files continue to grow in size and more information will be accessed remotely. There are dozens of examples in the home where bandwidth will be critical, such as the television programming, games and the Internet.

George Gilder writes in his book Telecosm, that eventually the nodes in the network will contain very little data. The bulk of the data will be stored in remote locations, available on demand. This will be very true in the home-networking environment. Much of the data will be accessed remotely, such as the programming that was previously mentioned. The family may download and keep a copy of their favorite music and movies, but a majority of it will be viewed and listened to once and discarded. There will not be a gigantic need for storage in the home, just access to bandwidth. Bandwidth will be provided by a physical medium that has a tremendous ability to pump data, such as fiber.

IPv4 Data Flow

The IPv4 header consists of a version, Internet Header Length, Type of Service, Total Length, Identification, Flag, Fragment Offset, Time to Live, Protocol, Header Checksum and Options field along with the Source and Destination address fields. Some of these fields have been dropped or made optional to keep the overhead to a minimum. Even though the IPv6 addresses are four times longer than the IPv4 addresses, the header is only twice the size of the IPv4 header (Goncalves, 1998).



(Huitema, 1998)

The header length field found in IPv4 is not necessary in IPv6 because all IPv6 headers are the same. IPv4 headers can be as short as 20 bytes and as long as 60 bytes. The IPv4 datagram length is the entire datagram including headers. Routers calculate the length of an IPv4 payload by subtracting the header length from the datagram length; IPv6 does not need to process this calculation.

The type of service is really made up of two sub-fields: precedence and type of service. Precedence is the level of priority and the type of service is more an indication for routing (Huitema, 1995). There were originally three types of service bits defined, a delay bit, a throughput bit and a reliability bit. These type of service bits were designed to compute a default route, the shortest route, the largest throughput or most reliable route (Huitema, 1995). The precedence indicator is used for queuing purposes. There are eight preference values, and works on the premise that the packet with the highest priority will be sent first.

The fragmentation and reassembly process uses the identification, flags and offset fields. When an IPv4 packet is fragmented it is given a complete IP header, which are copied from the original packet. If one fragment is lost the entire packet must be resent. In IPv6 only the source router does the fragmentation, in IPv4 fragmentation can be done at any intermediary node. In IPv6 all intermediary nodes ignore the fragmentation extension headers which improves efficiency as the packets are routed (Loshin, 1999).

In IPv4 the options are added to the end of the header, which means the options header is always taking up overhead. IPv4 options require that packets get special handling which slows down processing times (Loshin, 1999). In IPv6 the options are added by using a separate extension header. The option header is only processed when necessary. All IPv4 packets are treated the same by all the routers- the source routers, the intermediary routers and the destination router.

IPv6 Data Flow

IPv6 has some major changes over IPv4 when it comes to the header. With all of the additional tools available in IPv6, multimedia will become even more of a reality, or at least start to address some of the real expectations of multimedia. The timing issues and bandwidth requirements have been addressed with IPv6, and hopefully these features will have a profound impact on how multimedia is implemented in the future.

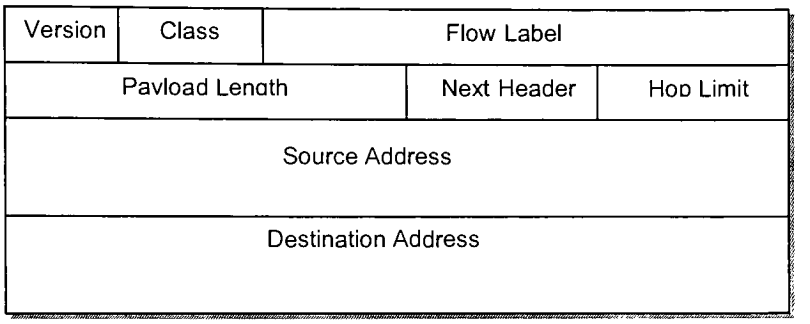
From a networking perspective, large amounts of traffic can cause delays and bottlenecks. One of the ways of dealing with vast amount of data is by maximizing the use of bandwidth. Multicasting addresses will help manage the flow of data effectively

and efficiently. Multicasting will be an easy solution to disseminating a large amount of data to many users without tying up valuable network resources. There are applications that will continue to emerge as a result of multicasting. It will be important to have the ability to join a newsgroup and a weather forecasting group. Even when it comes to conducting research such as the census, the many-to-one capability that multicasting offers will be a tremendous help. In addition, the data that is being sent doesn't have to be broadcast out into the entire world. It is only sent to the users who request it or need to receive it. An anycast addressing will give the ability for efficiency as well when it comes to keeping all of the clocks up-to-date.

Another important factor in multimedia is being able to handle large packet sizes. IPv6 accomplishes this by allowing packet sizes of up to 4 billion bytes. This means that IPv6 will be able to take advantage of all of the available bandwidth over any transmission media. These jumbo packets will require special treatment because not all of the links will be able to handle these very large packets and the routers will need to check at every node which is the best route to follow. These Jumbo payloads are any packet greater than 65,535 bytes (Hinden, 1999). This will be beneficial as backbones and capacity becomes less of an issue. Jumbograms allow any packet size necessary. Jumbograms can be used to send very large amounts of data, which is ideal in a scenario where the sending node needs to get the data out without interrupting the data flow. The other advantage of IPv6 is the source router will fragment the payloads prior to sending them into the network if sufficient bandwidth is not provided between the source and destination. IPv4 currently fragments the packets as it is traversing the network, which is not as efficient.

IPv6 headers

The IPv6 header, which is 40 octets, is approximately twice the size of an IPv4 header, but provides some simplification from the IPv4 header. All headers have a fixed format, there is no longer a checksum, and the hop-by-hop segmentation procedure has been removed. There are eight fields in the IPv6 header:



(Huitema, 1998)

1. Version (4-bits)
2. Traffic Class(8-bits)
3. Flow label (20-bits)
4. Payload length (16-bits)
5. Next header (8-bits)
6. Hop Limit (8-bits)
7. Source address (128-bit)
8. Destination address (128-bit)

The version field indicates the version of IP in use. The traffic class field contains a value that identifies the priority level for delivering packets. Each individual packet can have a different priority even if it originated from the same source. There are two ranges of priorities 0-7 and 8-15. Priorities 0-7 are reserved for low priority packets. If traffic is heavy, the packets will back off. These packets do not need to arrive in real time and can be delayed. Priorities 8-15 are used for non-congestion controlled or real-time traffic. The packets that are sent at 15 are critical for maintaining a constant rate, and

the packets at 8 are still real-time traffic, but the transmission would not suffer tremendously if the packet was lost (Goncalves, 1998).

The flow label gives the source the ability to label a sequence of packets, which requires the router to give the packets special handling. All packets belonging to the same flow must have the same source, destination, priority and flow label. A flow label can be used to establish routes that give better service, including lower delay or bigger bandwidth. Each and every packet that has flow labels changes the handling within the router, which can cause difficulties within the routers' cache.

The payload length defines the length of the packet following the header. The minimum payload is 576 octets with the ability to have payloads greater than 65,535 bytes, which are called jumbo payloads. This field identifies jumbo packets by setting the payload length to zero and then specifying the length in the hop-by-hop extension header.

The next header field identifies the header that is immediately following the IPv6 header. These extension headers are used to specify special case treatment of some packets. The extension headers could be an Authentication Header, an Encapsulation Security Header, a Routing Header, an Upper Layer Header, a Fragment Header, Destination Options Header or a Hop-by-Hop Options Header. There is a recommendation for the order these extension headers are placed in the IPv6 packet.

The hop limit identifies the number of hops the packet can travel from its source to the destination. This is a counter that decrements by one at each hop. Once the field

reaches zero, the packet is discarded. IPv6 has the ability to measure the maximum number of hops that can occur as the packet is forwarded. This replaces the Time to Live field found in IPv4, and no longer uses time as a component. The source address field contains the 128-bit address of the originator and the destination address field contains the destination address.

Multicasting

Multicast addresses have many applications in distributed systems such as home network environments. It allows for large groups of users to be identified and reached without wasting unnecessary bandwidth and time. In essence, a multicast address is an identifier for a set of interfaces that usually belong to different nodes (Goncalves, 1998). Instead of a broadcast message in IPv4 that sends the message multiple times, multicasting disseminates copies of the messages through a hierarchical method. It is very efficient at reaching subscribers that have been identified as a part of a group. Multicasting allows for users to join and leave groups very easily and supports video conferencing and push media. It can help in replication processes or distribute updates and announcements. It allows for seamless interaction between one-to-many, many-to-one and many-to-many.

Some may argue that multicasting is not necessary because it is not an issue to have the sender originate multiple copies. Broadcast messages accomplish reaching multiple users, however the message is not targeted specifically to the recipients. All of the receivers must examine the message to identify whether they are supposed to "pull" it off the network. This can cause a tremendous amount of wasteful processing time and energy. Multicasting gets right to the point. The homeowner would be able to notify the

sender that they would like to join the multicasting group and the messages are delivered succinctly and without waste.

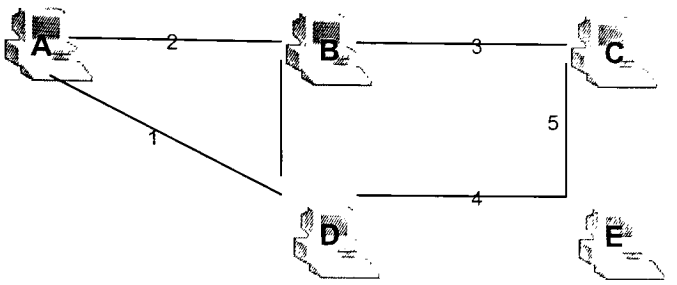
This type of information management becomes more and more useful when it comes to homes in the future. Information can be quickly disseminated on a regular basis with little input from the sender. This is helpful for a ubiquitous computing environment because very little interaction needs to occur in order to have current information sent and updated. Multicasting is very flexible, and doesn't require hour upon hour of intensive administrative work for maintaining groups.

Multicasting defined

In order to clearly define what multicasting is it is important to understand the differences between multicasting and multiple unicasting. In a unicast network, the sender or host will have to send out a single message to each recipient. This means each message will be handled by a router, or will take up bandwidth, and the sender is required to handle each transaction. The problem is amplified as the number of recipients is increased. For example, if a neighborhood had a weekly newsletter that they sent out to 50 recipients, the overhead required to manage this type of communication is not extreme. If the same newsletter were going to be sent to 500,000 homes across the globe, it would be an entirely different story. It is the same concept of sending out a note to each home in an individual envelope, versus sending one copy out and having it routed around until only the people who are supposed to receive it pick it up without delay.

An example of point to point or unicasting versus multicasting is shown below. In point to point four copies must be sent in order to send a copy to B,C,D, and E from A.

This each transaction will have to be carried over each link until it reaches the destination.



Using pt-	to-	pt				Multicast
For	B	C	D	E	Total	
Link 1			1	1	2	1
2	1	1			2	1
3		1			1	1
4			1		1	1
	1	**2**	**2**	**1**	**6**	4

Figure 4 (Huitema, 1995)

Multicasting applications

One-to-Many applications are traditionally thought of as broadcast types of applications such as TV and radio, but in reality there are many more applications that can be supported by this type of interaction. These applications can include scheduled audio/video conferences or push media, which are items such as weather forecasts, news headlines or other data that is periodically updated. Caching can also benefit from multicasting- replication processes or other file-based updates. Announcements such as time, keys, configuration updates, locality beacons or other types of commonly required information. This also can be used for monitoring purposes, such as stock prices, security systems or other real time data. Resource discovery also falls under the One-

to-Many category. Resource discovery can be used to find the closest host or other types of data.

The Many-to-One applications are the reverse of One-to-Many. For example data points could send data back to a single node for collection and analysis. Auctions could also be conducted in this manner- each node could silently or privately send in their bid. The census polls could work in the same vein. The question is posted and the individuals could respond. The other large use of multicasting will come from Many-to-Many applications. This is the more traditional multimedia conferencing, distance learning and multi-player games. Many-to-Many applications also include easily synchronizing resources, such as calendars and schedules, concurrent processing, collaboration, and chat rooms (Quinn, 1998)

There are many uses for multicasting yet to be discovered. As bandwidth increases, we will be able to accomplish more and more collaboration from farther points around the world. Multicasting will enable ubiquitous computing to become a reality. It will allow simultaneous weather and traffic updates to be available while a cup of coffee is consumed. Homes can belong to a demographic group, or a neighborhood group or a city group with very little management and input.

As networks start to move into the homes in the future, it is also important that security is maintained and improved. With multicasting there are ways to limit the number of users that can see the data intended for a certain group. Instead of sending a message out to the entire world and having the ability for anyone pick up a message, multicasting eliminates the need to send the data to every node, it is only routed to the

defined host groups. The protocol and routers will know where the message is needed. Multicasting will help the dissemination of information to households all over the world. Multicasting is perfectly suited for applications in the home of the future.

Quality of Service

IP has mostly been used for data applications that are suitable for a best effort delivery system. Streaming video and voice has not been widely distributed via the Internet because of bandwidth limitations and the lack of Quality of Service (Qos). QoS is important for mission-critical applications, for integrating voice and data networks, and giving the routers and switches the ability to handle more packets per second. Most firewalls limit the size of file attachments because of the routers have a limited ability to handle large file transmissions. In addition, there has been no efficient way to prioritize packets that are time sensitive, such as voice and video. This is critical as the congestion increases because packets can be lost or delayed, dramatically effecting the transmission quality. There have been a couple of methods developed to improve IP's ability to deliver time sensitive packets with little to no delay.

Reservation protocols are used to reserve resources in the network to ensure packets will arrive in a timely and orderly fashion. Resource reservation protocol (RSVP) discovers the route of a specific flow and then sends the remaining packets down the same route. Packets will not be dispersed over multiple routes allowing packets to arrive out of order and at different times. A reservation, or flow specification is made to reserve a route so the packets can be sent with appropriate throughput and minimizing delay. A path message is used to identify the next hop from the origination to the destination. The path messages and reservations will continually be refreshed during

the RSVP 'session', so when the routing tables are updated the path will be updated as well. Just as there are path and reservation requests, there are path and reservation tear down requests that are sent to free the resources once the session is completed. There are some major issues with scaling RSVP because RSVP requires that routing decisions are made at each intermediate node along the path (Stephenson, 1998). Each router has to maintain the reservation information and know where the next hop is in the path. RSVP has not been widely adapted.

Diffserv uses the IPv4 Type of Service field to specify the service requirements. The ToS field is referred to as DS byte. It is implemented in Layer 3 by upgrading firmware or software in routers. Diffserv uses the ToS field to identify service level requirements by the packet not by the session. QoS will be maintained by the DS byte specifying the traffic flow and maintaining the appropriate bandwidth levels. The traffic flow is specified by using traffic conditioners that manages queues, groups packets based on the type of service and identifies packets that will be the first to be dropped when congestion occurs. Packets that are time sensitive are sent to queues that are shorter and expect less delay.

MPLS (Multiprotocol Label Switching) is used to specify how Layer 3 traffic can be mapped to connection orientated Layer 2 transports (Stephenson, 1998). MPLS requires label-switching routers that read header information because the IP traffic is encapsulated with new routing headers. The MPLS label identifies the QoS and the path of the packet. As the packet traverses the network it may need to be relabeled based on the ability to maintain the shortest path. MPLS simplifies the routing process by specifying the packet's path, which frees the router from having to process the next

hop. The MPLS label has already identified the next hop. In addition, the QoS only needs to be read once at the edge of the network because the level of QoS needed identifies the appropriate path.

Cisco has developed a tag switching architecture that will allow networks to handle more traffic, media rich data and bandwidth intensive applications in multilayer environments (Cisco, 1999). This is a routing architecture that is based on the concept of label swapping, which will improve IP scalability. Tagging is accomplished by associating a tag with the first flow of data that will allow subsequent packets to be expedited to the final destination.

There will be some changes with IPv6 in regards to Quality of Service, however a majority of the QoS protocols that will be implemented with IPv4 will also be implemented with IPv6, such as RSVP, Diffserv, MPLS and Cisco tags. Instead of the Type of Service field in IPv4, IPv6 will use the flow header and traffic class header to define the QoS and flow specifications. IPv6 will be more efficient in handling QoS traffic.

As QoS becomes more important with the Internet Protocol new specifications will continue to develop. Flow labels will let many packets be transmitted over a connectionless system and reassembled in order so there will be lower delay and greater bandwidth. Routers will handle these packets differently so they can deliver data for applications such as video conferencing and multimedia. Packet priority will work in conjunction with the flow labels because it can differentiate the asynchronous data from the isochronous data. It is now possible to handle large portions of data quickly and

efficiently over a connectionless network. This type of data transfer is necessary for streaming data, which has many uses for multimedia, gaming and the telephone.

These types of technology will allow more flexible control of how packets are routed, which will help in developing in a routing system that will accommodate the emerging applications. Although these types of architectures are likely to be implemented in Wide Area Networks, eventually this type of efficient flow control will become integrated into a LAN environment. Improving IP's ability to effectively and efficiently route packets requires finding new architecture in both WANs and LANs. It is not built into the protocols basic functionality, but must be added as overhead. IPv6 will have some advantages IPv4 in regards to data flow because Ipv6 will be able to handle the Quality of Service more efficiently and will use the network resources more effectively. IPv6's flow header and traffic class header will be more efficient than the Type of Service field found in IPv4. However, the same types of Quality of Services will be implemented.

Summary

The Internet has already made an impact in U.S. households, but it is only the beginning. The quality of life in our homes will improve. The Internet, or some form of it, will be useful and viable in the home network. The Internet will dominate as the primary resource for sharing data as networks of the future become more powerful and robust. It will be a vast matrix of wireless and wireline devices; all trying to create a seamless system of information that will improve our lives. There are many aspects of a seamless communications system, and one of the most important aspects is the ability to interface physical networks with multiple operating systems. The Internet Protocol is merely

software designed to be this interface. Users, applications programs and higher layers of protocol software use the Internet Protocol addresses to communicate (Comer, 1997). It is the essence of the communication that occurs throughout the Internet.

The Internet Protocol remains important for several reasons. It is non-proprietary, open, and it offers ways to merge voice and data traffic on a common platform. IP networks meet the requirements for interoperability and integration, scalability, reliability, mediation, manageability, security, and have global reach (Muller, 1998). Each version of the Internet Protocol has similar characteristics and abilities. A majority of the features in IPv6 are not new. Internet Protocol version 6 retains all of the positive aspects of IPv4, but incorporates all of the lessons that has been learned over the last twenty years. IPv6 has taken advantage of IPv4's history and will be the only protocol that will meet the needs of home networks in the future.

It is necessary to consider the possibility that more IPv4 enhancements could extend IPv4's life expectancy. There may be more solutions that have yet to surface that could keep IPv4 firmly entrenched. There may be problems with implementing IPv6 that have not been uncovered. It is also possible that there may be other layers that could be improved to keep IPv4 viable. IPv6, however, has many features that will be better in a home networking environment than IPv4. Ipv6 will The other option is that IP does not survive and is replaced by an entirely different protocol, however this is highly unlikely.

Volume

IPv4 is limited to 4.2 billion devices communicating on the global network at any given point in time. Eventually it will not be enough. The volume of devices will increase

dramatically as smart devices are developed and incorporated into our homes. Although not every household on the planet will have the need for multiple devices connected to a global network, the number will grow beyond IPv4 capabilities. Many homes today have a computer with an Internet connection, but this does not resemble the home networks of the future. Home networks will have a high density of nodes and will consist of many complex systems made up of many individual devices. The average on-line home may have an average of 45 devices that are all able to communicate.

IPv4 will not be able to sustain the volume of devices that will be needed. Eventually CIDR will not provide the level of aggregation required, and NAT will not support all of the new options available. NAT already has limitations with IPSec, which is gaining more popularity because of VPNs. NAT is just a temporary solution to an existing problem; it is not a long-term solution. CIDR is still not supported in all parts of the Internet. Even if the addresses were not completely depleted the addresses would still need to be managed carefully. It is already difficult to manage a depleting address space and will only become more difficult in the future. It might require reassigning millions of addresses. It isn't feasible in an environment where there would be billions of people affected. With IPv6 there are 32 addresses per square inch of dry land and at the current time only 15% of the addresses have been designated

IPv6 has enough capacity to handle all the needs of home networks and the commercial sector. In addition to address space, the IPv6 design choices were made to insure default-free routing tables are manageable in size and the examination of packets is kept to a minimum as the Internet grows in complexity and size. Aggregation and well-planned dissemination of IP addresses will help cut down on the routing tables.

Ideally IPv6 address aggregation will be managed at the ISP level. Table aggregation is very well thought out with IPv6, and will hopefully ease a lot of the routing table issues. Maintaining efficiency is extremely important. IPv6 will use addresses more efficiently because the addressing scheme is based on interfaces, not nodes. Fully implemented multicast addresses would also ensure that Internet resources would not be wasted. Table Aggregation, multicast and a 128-bit addressing scheme will be the only solution for moving forward.

Ease of Use

A majority of homeowners do not have the ability to configure an IPv4 network. In some cases networks of today require inputting IP addresses, host names, subnet masks, default routers, DNS server address and other types of parameters. It can be complicated, costly and a time-consuming process. This will not be acceptable. Consumers of every age, intelligence and size should be able to manage all of the components in the household. The devices need to immediately become a part of the home networking environment with little to no input on behalf of the owner. A device should have the ability to determine what other devices are in the general vicinity and how to communicate within the environment.

One of the keys of success in home networks will be simplicity. Simplicity in the way the system works, how it is installed, and how it is maintained. Complexity needs to be entirely transparent in order for the technology to be adopted into the home. It is important to be able to handle a high density of nodes with different data transfer requirements. IPv6 is simpler than IPv4 for a couple of reasons. The designers had twenty years of experience before IPv6 was designed. There has been time to identify

the weaknesses in IPv4 and make corrections. Some of the solutions have already been defined and implemented in IPv4. IPv6 was designed knowing it was going to be changing and evolving over time, therefore the flexibility has been written into the protocol. IPv6 has extension headers and ways to incorporate enhancements in the future without having to make major changes to IPv6 infrastructure. As more enhancements are added to IPv4, the more difficult it will be to manage. Although there is a lot of resistance to adopting IPv6, it will create a simpler network.

Although IPv4 has DHCP, which allows the device to do a network query to determine its address, it still does not have all the capabilities of IPv6. Most of the autoconfiguration done today is supported by the operating systems. Most programs or hardware installations use a wizard to walk the user through the configuration process. There are few situations where a peripheral device is completely functional by plugging it into the wall. IPv4 was not intended to be utilized in a user-friendly environment. It was primarily designed for stationary and static devices. The homes of the future will have devices that are constantly being added and moved. IPv4 is not as efficient as IPv6, which means resources will be unnecessarily wasted. IPv4 will not be able to support plug and play as well as IPv6.

IPv6 supports automated address changes, mobile hosts, and dead neighbor detection. Neighbor discovery in IPv6 replaces ARP, ICMP Router Discovery messages and ICMP Redirect messages in IPv4. Nodes are able to determine neighbor's link-layer addresses as well as purge addresses that have become invalid. Neighbor unreachability detection allows mobile devices to leave the network without causing other links to fail because the change is quickly detected. Router discover is part of IPv6

base protocol set instead of requiring additional packet exchanges that take place in IPv4 networks. Multicast addresses are also used in the address resolution process, which is much more efficient because it does not affect nodes unnecessarily. When less overhead packets are necessary the network is working more efficiently and systems are configured more quickly. IPv6 allows devices to essentially manage themselves with little interaction. IPv6 was designed to be plug and play compatible, and will definitely be advantageous in home networks.

Security

When IPv6 was in the process of being designed, security was one of the top issues. Data transfers need to be secure at every layer. This is especially true in homes. Security needs to be present inside and outside of the house. Homeowners will not accept outsiders being able to monitor the activity inside the home.

Fortunately, IPsec will be implemented in both IPv4 and IPv6. As IPSec has been developed for IPv6, it has been implemented in IPv4. There are very few differences between the two protocols when it comes to security. Home networking environments will benefit form the ability to authenticate, encapsulate and encrypt packets. It will allow transmissions inside and outside the home to be maintained with high levels of security.

Data flow

Home networks will require all Types of Service and levels of Quality of Service because of the range of applications found in a home network. Isochronous and asynchronous data flows will be constantly needed. The key to effective data flows is

the ability to efficiently handle packets. The network performance will be optimized because the routers will be handling the packets less

Data flow is not as efficient in IPv4. The IPv4 headers vary in size, which means the routers have to calculate the length of an IPv4 payload, which creates additional overhead. Fragmentation occurs at intermediary nodes, whereas IPv6 fragments at the originating node. Any time an option is added to the header it takes up additional overhead and also creates inefficiencies because each router has to analyze the header. IPv4 was not designed to handle the needs of voice, video and other applications that need quality of service. . Streaming video and voice has not been widely distributed via the Internet because of bandwidth limitations and the lack of Quality of Service (Qos).

IPv6 makes better use of overhead than IPv4. The headers have been optimized because they were designed to use extension headers instead of options, maintain a constant header size, redefined packet fragmentation and reduced the amount of special handling needed for individual packets. Multicasting will also allow IPv6 to more efficiently use bandwidth than IPv4. Homeowners will have to ability to easily join and leave groups and services with minimal impact on the network. Information can be easily exchanged with very little interaction required by the user. Although some aspects of Quality of Service will be the same for IPv4 and IPv6, IPv6 is designed to easily integrate changes and IPv6 already has these capabilities as part of the base protocol. The enhancements available today will continue to be tested and designed to improve capabilities in the future.

Conclusion

The homes of the future will require new levels of computing capabilities. Instead of a stand-alone personal computers there is a potential for several smart devices and appliances in each room in the home. It is expected in places where there are one or two computers today, there will be a hundred computers and the same number of networks required. The number of devices will increase beyond the capacity needed today. Home networks will need to handle many nodes. In the average room there may be 10-15 devices interacting with each other. Multiple nodes in the home will access the Internet. Data will constantly gathered and updated throughout the entire systems.

The Internet Protocol is a perfect solution to the needs and demands for the data flows and exchanges needed in the future home networks. IP has the ability to manage the interaction of devices within the network and out to the Internet. It has the flexibility to cross all platforms and connect systems at every corner of the world. It can handle asynchronous data and isochronous data such as Voice over IP. There is no doubt that IP will be an important part of the home networks in the future.

There are four main areas of home networking that are the most important; the increased volume and high density of devices, security, ease of use and data flow. These four features are critical for the home-networking environment. Security will have to be fail-safe. It is important that privacy is protected. Adding new devices must be seamless. The amount of data that will flow in and out of the homes will greatly increase. There are many applications such as video conferencing, multimedia and other forms of entertainment that will require not only large amounts of bandwidth, but also the ability to stream data without delays.

IPv4

Some of the features that have been fully developed in IPv6 could potentially be incorporated into IPv4 with one major exception, address space. Exhaustion of the class B addresses, routing table explosion and address depletion are issues with IPv4 that have temporarily been solved, however, the solutions are just temporary. At some point in time it will be necessary to find a replacement for IPv4 based strictly on the number of devices accessing the global network all at the same time. Without the additional addressing space, this will not become a reality. The number of components will continue to expand as more people start to depend on microprocessors. Even if new addressing schemes such as NAT and CIDR are implemented, it still will be necessary to take the next step. IPv6 will be essential to the full implementation of ubiquitous computing in the home environment.

IPv4 does not have the level of sophistication that IPv6 has for ease of use and autoconfiguration that home networks require. A ubiquitous computing environment requires that all of the devices have the ability to immediately integrate into the network. Most plug and play implementations with IPv4 are driven by the operating system, not the protocol.

IPv4 does have the same capabilities as IPv6 regarding security. The IPv6 security initiative has also enhanced IPv4. Although quality of service is possible with IPv4 it does not have the ability to be as efficient as IPv6. In most cases IPv4 enhancements to quality of service would require extensive upgrades and changes to the protocol. Even with an upgrade, IPv6 has far more capabilities than IPv4.

IPv6

IPv6's 128-bit addressing will sustain address needs for many decades to come. In addition, IPv6 takes advantage of more efficient routing tables by incorporating table aggregation and fully implemented multicasting capabilities. IPv6 was designed knowing the potential networking needs. The IP addressing scheme utilizes "longest prefix match", which means the routers only need to examine the part of the address that is needed to get to the next node. The routers can be more efficient.

IPv6 also incorporates autoconfiguration and ease of use into the protocol. Devices will be able to determine where it resides on the network and obtain other pertinent information. IPv6 supports automated address changes, mobile hosts and dead neighbor detection. Address resolution and neighbor discovery are more efficient than in IPv4. Router discovery is part of the base protocol; no additional packet exchanges are necessary. IPSec is a security architecture that was designed for Internet Protocol version 6. It allows authentication and maintains the integrity and confidentiality of the IP packets. Fortunately IPSec has already been incorporated into IPv4.

IPv6 will address the issue of data flow by effectively utilizing multicasting addresses, jumbo packets, flow labels, traffic classes and extension headers. In addition, all of the Quality of Service methods can be easily implemented into IPv6. IPv6 will be ready to address the needs of all the applications that will be found in the home.

Depending on how well v4 interoperates with IPv6, IPv4 may continue to exist within mixed IPv6/IPv4 networks for a long time (3Com, 1998). Some experts suggest

that IPv4, with its IPv6-like feature enhancements, will suffice for more than a decade (McNealis, 1998). IPv6 is robust and standard, however, and it will almost inevitably make up the Internet backbone of the future (Faulkner, 1998). Home networks will not become a reality for at least a few more years. It is the perfect time to be an advocate for preparing these newer networks to be IPv6 compatible, and in some cases one hundred percent IPv6. In many respects the features of IPv6 will be required in a home-networking environment as previously stated. These enhancements include packet prioritization, flow labeling, neighbor discovery, auto configuration, security and real-time application support.

Home networks will someday be a reality. They may not be as far fetched as some can imagine, but they will not be immune to the ever growing need for people to rely more and more on technology. Ubiquitous computing will reach new heights as the years unfold. In order to make this happen there must be a symbiotic relationship between all of the devices and appliances and the rest of the world. Internet Protocol version 6 is the only Internet Protocol that will make the home networks of tomorrow a reality.

Some of the features that have been developed in IPv6 could be incorporated into IPv4 with one major exception, address space. At some point in time, it will be necessary to find a replacement for IPv4 strictly based on the number of devices that will be accessing the global network all at the same time. Without the additional address space, home networks will not become a reality. The number of components will continue to expand as more and more people start to depend on microprocessors. IPv6

will be essential to the full implementation of ubiquitous computing in the home environment.

Sources

Text books:

1. Cairncross, Frances (1997). The Death of Distance- How the Communications Revolution will Change Our Lives. Harvard Business School Press. Boston, Massachusetts.

2. Comer, Douglas (1997). Computer Networks and Internets. Prentice Hall, New Jersey.

3. Gershenfeld, Neil (1999) When Things Start to Think. Henry Holt and Company, New York.

4. Gilder, George (1997). Telecosm. Simon & Schuster.

5. Goncalves, Marcus and Niles, Kitty (1998). IPv6 Networks. McGraw-Hill, New York.

6. Huitema, Christian (1995). Routing in the Internet. Prentice Hall, New Jersey.

7. Huitema, Christian (1998). IPv6- the New Internet Protocol. Second Edition. Prentice Hall, New Jersey.

8. Loshin, Pete (1999). IPv6 Clearly Explained. Morgan Kaufman, San Francisco.

9. Malone, John (1997). Predicting the future: From Jules Verne to Bill Gates.

10. Miller, Mark A. (1998). Implementing IPv6. M&T Books, New York.

11. Negroponte, Nicholas (1996). Being Digital.

12. Plunkett, John (1996). Mind Grenades, Manifestos from the future.

13. Weiners, Brad and Pescovitz, David (1996). Reality Check.

Other sources:

1. 3COM (1998). IPv6: Next Generation Internet Protocol. Retrieved from the World Wide Web on March 39, 1999. Available on-line: http://www.3com.com/nsc/ipv6.html

2. Adhikari, Richard (1999, Aug. 18). IPv6: Just Say No! PlanetIT World Wide Web site. Retrieved from the World Wide Web on August 24, 1999. Available on-line: http://www.planetit.com/techcenters/docs/advanced_ip_services/opinion/PIT19990816S0013

3. Cisco World Wide Web site. (1999). Retrieved from the World Wide Web February 6, 1999. Available on-line: http://www.cisco.com/warp/public/732/ipv6/index.html

4. Cooperstock Jeremy Fels, Sidney. Buxton, William. Smith, Kenneth. (1997 Sept.). Reactive Environments. Association for Computing Machinery. Communications of the ACM [Online] Vol. 40, Issue 9. Pages 65-66. Retrieved from the World Wide Web on September 29, 1998. Available on-line: http://www.acm.org

5. Dickinson, John (1999, April). The future is...home networking. Home Office Computing. Vol 17, Issue 4, Start page 4. Retrieved from the World Wide Web on April 30, 1999. Available on-line: https://www.rit.edu:8080/_proxy_/proquest.umi.com/pqdweb?ReqType=301&UserId=IPAuto&Passwd=IPAuto&JSEnabled=1&TS=925847426

6. Electronics Now (1998, December). Home-networking standard. Electronics Now. Vol. 69, Issue 12, Start page 16. Retrieved from the World Wide Web on April 30, 1999. Available on-line:www.proquest.umi.com

7. Faulkner Information Services (1998). Implementing IPv6. Retrieved from the World Wide Web February 6, 1999. Available on-line: https://www.rit.edu:8080/_proxy_/www.faulkner.com/products/faccts/default.htm

8. Francis, P. (1994, May). Request for Comments: 1631. The IP Network Address Translator (NAT). Cray Communications. Retrieved from the World Wide Web on August 27, 1999. Available on-line: http://194.52.182.96/rfc/rfc1631.html

9. GlobalStat (1999). Global Statistics- Europe. Retrieved from the World Wide Web on June 17, 1999. Available on-line: http://www.stats.demon.nl/

10. Greenberg, Ilan (1997, Dec 8). The future of the living room. Cnet News.com. Retrieved from the World Wide Web April 29, 1999. Available on-line: http://cnet.com/Content/Features/Dlife/Living/index.html

11. Hall, Eric (1997, February 15). Hide and Seek with Gateways and Translators. EHS Company. Retrieved from the World Wide Web August 27, 1999. Available on-line: http://www.ehsco.com/reading/19970215ncw1.html

12. Haring, Bruce (1998, Oct 7). Coming soon: cooperating appliances. USA Today. Page O5D. Retrieved from the World Wide Web on April 30, 1999. Available on-line:www.proquest.umi.com

13. Harris, David (1998, Dec 29). Position statement on applications. Retrieved from the World Wide Web on April 30, 1999. Available on-line: http://www.pa-fiber.net/issues_applications.htm

14. Hawley, Mike (1996, April). Statement of research. Personal Information Architecture, MIT Media Lab. Retrieved from the World Wide Web May 25, 1999. Available on-line: http://www.media.mit.edu/pia/info.html

15. Hinden, Robert (1999). IP Next Generation (Ipng). Retrieved from the World Wide Web April 21, 1999. Available on-line: http://playground.sun.com/pub/ipng/html/ipng-main.html

16. Huffstutter, P.J. (1998, Nov 2). The cutting edge; IBM gets in on ground floor of state's 'smart' home market. The Los Angeles Times. Page 3. Retrieved from the World Wide Web on April 30, 1999. Available on-line:www.proquest.umi.com

17 Intel World Wide Web site (1999). Home networking from Intel. Retrieved from the World Wide Web April 1, 1999. Available on-line: http://www.intel.com/anypoint/home.htm

18. Internet RFCs http://www.cis.ohio-state.edu/hypertext/information/rfc.html

19. Internet Engineering Task Force (IETF) http://www.ietf.org/

20. Internet drafts (by FTP) ftp://ds.internic.net/internet-drafts/

21. Kaye, Joseph and Krikorian, Raffi (1997, April). Personal Information Architecture Group. Retrieved from the World Wide Web May 25, 1999. Available on-line: http://www.media.mit.edu/pia/Pubs/AprilDemo/opening.html

22. Kessler, Gary (1997, February). IPv6: The Next Generation Internet Protocol. Retrieved from the World Wide Web February 6, 1999. Available on-line: http://www.hill.com/library/ipv6_exp.html

23. Leopold, George. (1996, Sept. 23). 'Ubiquitous' computing hits a wall. Electronic Engineering Times [Online]. Issue 920. Page 1. Retrieved from the World Wide Web on September 29, 1998. Available on-line: http://www.acm.org

24. Marshall, Jonathan (1998, Jan 29). Wired for the future/Demand grows for houses with networks. San Francisco Chronicle. Final Edition, Page E1. Retrieved from the World Wide Web May 3, 1999. Available on-line:www.proquest.umi.com

25. McNealis, Martin (1998). IP Crossroads- migrate to IPv6 or evolve with IPv4. Packet Magazine Archives. Retrieved from the World Wide Web February 6, 1999. Available on-line: http://www.cisco.com/warp/public/784/packet/july98/9.html

26. Merloni Elettodomestici World Wide Web Site (1999). Ariston Digital- The new generation of appliances. Retrieved from the World Wide Web May 11, 1999. Available on-line: http://www.merloni.com/eng/ari_digi.htm

27. Miles, Stephanie (1999, April 29). Intel peers into the home of the future. CNET News.com. Retrieved from the World Wide Web May, 11, 1999. Available on-line: http://4a2z.com/cgi/rfr.cgi?http://www.news.com

28. Morrison, Gale. (1998, April 6). Embedded challenge: Software to the rescue. Electronic News [Online]. Vol. 44, Issue 2213. Page 6. Retrieved from the World Wide Web on September 29, 1998. Available on-line: http://www.acm.org

29. Mouhanna, Joseph (1999, May 14). In-Home Networks: Making things talk. Connections '99 conference, Vancouver BC.

30. Muller, Nathan (1998). TCP/IP Networking Protocols. Retrieved from the World Wide Web February 6, 1999. Available on-line: www.faulkner.com

31. Muller, Nathan. (1999). Home networking market trends. Faulkner Information Services. Retrieved from the World Wide Web April 30, 1999. Available on-line: www.faulkner.com/products/faccts/default.htm

32. Muller, Nathan. (1999). Introduction to home networking. Faulkner Information Services. Retrieved from the World Wide Web April 30, 1999. Available on-line: www.faulkner.com/products/faccts/default.htm

33. Number of Hosts advertised in the DNS (1999, January). Internet Domain Survey. Retrieved from the World Wide Web June 7, 1999. Available on-line: http://www.nw.com/zone/WWW/report.html

34. Office for National Statistics (1998, Sept 17) Household numbers and projections. Retrieved from the World Wide Web June 18, 1999, 1999. Available on-line: http://www.ons.gov.uk/ons_f.htm

35. Oosthoek, Simon (1997). Multicasting. Retrieved from the World Wide Web on April 13, 1999. Available on-line: http://www.huygens.org/people/oosthoek/thesis2/node17.html

36. O'reilly World Wide Web site. IP multicast protocol. Retrieved from the World Wide Web on April 13, 1999. Available on-line: http://www.ora.com/reference/dictionary/terms/I/Internet_Protocol_Multicast.htm

37. Poor, Robert D. (1997, Oct) High-Density Networks. Personal Information Architecture Group, MIT Media Laboratory. Retrieved from the World Wide Web May 25, 1999. Available on-line: http://www.media.mit.edu/pia/Pubs/HyphosSlideShow/

38. Quinn, B. (1998, November). IP Multicast Applications: Challenges and Solutions. Internet Engineering Task Force. Retrieved from the World Wide Web on April 13, 1999. Available on-line: http://www.ipmulticast.com/

39. Reinhardt, Andy and Licking, Ellen (1999, Feb 1). A smarter path to smart appliances. Business Week. Issue 3614, Page 67. Retrieved from the World Wide Web on April 30, 1999. Available on-line:www.proquest.umi.com

40. Residential Network Technology (1999). Presented at Connections '99. Training Department, Tucson, AZ.

41. Restivo, Kevin (1999, April 9). OSG fuels home networking. Computer Dealer News. Vol 15, Start page 38. Retrieved from the World Wide Web on April 30, 1999. Available on-line: Available on-line:www.proquest.umi.com

42. Reuters (1998, Oct 27). Smart devices, like Windows CE, to outsell home PC's by 2001. Yahoo News. Retrieved from the World Wide Web on April 30, 1999. Available on-line: http://www.palmsizepc.com/oct27-1.html

43. Request for Comments. Retrieved from the World Wide Web on May 4, 1999. Available on-line: http://www.rfc-editor.org/isi.html

44. Scott, Christopher and Scaduto, Teri (1998, Aug). Gizmo: CEMA okays home networking standard. Popular Electronics. Vol. 15, Issue 8, Page 26. Retrieved from the World Wide Web on April 30, 1999. Available on-line: Available on-line:www.proquest.umi.com

45. Solomon, Deborah (1999, April 26). Broadcom Buys Epigram in race for home networking/multiole devices to share single Net connection. Retrieved from the World Wide Web on April 30, 1999. Available on-line: Available on-line:www.proquest.umi.com

46. Stardust Technologies (1997). How IP Multicast Works. IP Multicast Initiative. Retrieved from the World Wide Web on April 13, 1999. Available on-line: http://www.ipmulticast.com/

47. Stardust Technologies (1997). Introduction to IP Multicast Routing. IP Multicast Initiative. Retrieved from the World Wide Web on April 13, 1999. Available on-line: http://www.ipmulticast.com/

48. Stardust Technologies (1997). Implementing IP Multicast in different network infrastructures. IP Multicast Initiative. Retrieved from the World Wide Web on April 13, 1999. Available on-line: http://www.ipmulticast.com/

49. Stephenson, Ashley (1998, Nov 21). Diffserv and MPLS: A Quality Choice. CMP's tech web. Retrieved from the World Wide Web on October 20, 1999. Available on-line: http://www.data.com/issue/981121/quality.html

50. Sun Microsystems. (1999, January 25). Sun unleashes Jini connection technology, smashing traditional network connectivity barriers for good. Retrieved from the World Wide Web May 24, 1999. Available on-line: http://wwwwswest2.sun.com/smi/Press/sunflash/9901/sunflash.990125.2.html

51. Talley, Brooks (1998, Oct 26). Appliances get smart. InfoWorld. Page 88. Retrieved from the World Wide Web on April 30, 1999. Available on-line:www.proquest.umi.com

52. Thomas, Susan Gregory (1997, Dec 1). The networked familty. U.S. News and World report. Retrieved from the World Wide Web on April 30, 1999. Available on-line: http://www.usnews.com/usnews/nycu/tech/tenetwor.htm

53. Thomas, Susan Gregory (1998, Aug 10). Home network. U.S. News & World Report. Vol 125, Issue 6, Pages 57-59. Retrieved from the World Wide Web on April 30, 1999. Available on-line: Available on-line:www.proquest.umi.com

54. United Nations (1998) Population Division. Department of Economic and Social Affairs. Retrieved from the World Wide Web on June 10, 1999. Available on-line: http://www.popin.org/pop1998/1.htm